Essays on Information Security Management from Internal and External Security Requirements: Empirical Examinations

Krannert Graduate School of Management

Purdue University

by

Juhee Kwon

October 2009

Contents

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

This doctoral dissertation proposal empirically studies how a firm can achieve successful information security management on both internal and external enterprise environment. As information assets have become a critical factor for enterprises to stay competitive, there is an increasing awareness of information security management. However, they are easily overlooked by those who focus only on the IT side, failing to see that human resources and policies are the most likely cause of information risks, which need to become real enterprise-wide and strategic issues. Therefore, this proposal first compares IT executive structural status across firms for achieving successful information security management in order to align it with the corporate governance approach, and the risk management policies within the organization. Then, it investigates how customers respond to firms' information privacy policies and how a firm motivates customer willingness to establish a long-term relationship by providing their personal information. These studies can give firms new insights into how they internally set IT executive compensation strategies as well as delegate authority and responsibility for ensuring confidentiality, integrity, and availability of information assets. Then, it sheds light on how firms can externally set up their practices for customer willingness to invest in a long-term business relationship by providing personal information.

Chapter 1 . Introduction

While information technology provides for powerful selling or buying power due to information richness, its digitally mediated communications make information security the most pervasive concern. Information needs to be accurate and up-to-date to enable an enterprise to make good business decisions and it needs to be available when the business requires access to it. As market relationships continue to change, information is more than ever, rapidly becoming the key business differentiator. Therefore, enterprises need to understand that they can be significantly disadvantaged by any risk to information security. The risks are enormous, but are easily overlooked by those who focus only on the IT side, failing to see that human resources and policies are the most likely cause of any risk in security. Information security needs to become a real enterprise-wide and strategic issue, taking it out of the IT domain and aligning it with the corporate governance approach and the risk management policies within the organization. Information security is not a 'nice to have' but a 'must have'. Enterprises must run their businesses to enable them to maintain the confidentiality, integrity and availability of information assets as a competitive edge in the tough market in which they operate.

Information security management has recently become a thriving and fast-moving research area. Researchers and practitioners have strived to understand and assess information security risks in order to find how to cope with the risks in competitive market structures. In practice, a recent survey showed that an enterprise's information security incidents significantly resulted in damage to reputation and brand by 85% of respondents (Ernst & Young, 2008; Young, 2008). The growing proliferation of

information security incidents is raising doubts about the Internet's future. Information security has become a priority investment in public and private organizations. It is also a known fact that the important strategic role of information security is only really established in a company once senior management gives it full support and commitment. Information security has long ago moved away from being only a technical issue, and has really today become a management issue.

Therefore, this proposal approaches the issues of information security from two different perspectives in order to provide insights about (1) how an enterprise can set IT executive compensation strategies as well as delegate authority and responsibility for Information Security Governance, and (2) how customers respond to an enterprise's information privacy policies and how customers' responses are related with an enterprise's actual accomplishment.

In the first essay, we examine the effects of an IT executive's structural status in Top Management Teams (TMTs) on information security risk management. *E*-Business has made it imperative for IT executives to adopt cross-functional roles due to the increased importance of securing and managing risks to information assets across the enterprise. Therefore, IT executive representation and status in a TMT is necessary to strategically and operationally conduct liaison activities between IT groups and other business units. However, there is little empirical research examining the effects of IT executives' structural status on managing information security risks. We employ logistical regression to examine 1148 firms from 2003 to 2008 with information security breach reports and executive compensation data. We augment this data with IT internal controls information

provided by external auditors. Our results demonstrate high IT executive engagement and fair compensation are associated with reduced levels of both IT internal controls weaknesses and reported information security breaches. Second, we find that pay dispersion in a TMT increases the probability of information security breaches, while IT executive turnover is not significantly associated with breaches. As a comprehensive analysis across the accounting, human resources, and information systems literature, this study gives firms new insights into how they set IT executive compensation strategies as well as delegate authority and responsibility for ensuring confidentiality, integrity, and availability of information assets.

The second essay studies the relationship among an enterprise's information privacy and security practices, and customer perceptions. Then, it also identifies how customer perceptions influence an enterprise's actual accomplishment and customer satisfaction. The Internet has presented a new framework for customer relationships and transactions, making it possible to map patterns of consumer behavior by getting close to the consumer over the Internet. Even though information security and privacy issues have been studied for many years throughout marketing and information systems literature, there have been very few studies dedicated to empirically examining the impacts of the interdependence among customer perceptions about a firm's security and privacy policies, and the firm's actual accomplishment. The purpose of our paper is to study how customers respond to a firm's various practices on security and privacy as well as how customer perceptions affect a firm's actual accomplishment and customer satisfaction. The results demonstrate

the effects of the firm's information security and privacy practices on customer perception, satisfaction and financial performance.

This dissertation provides two different perspectives studying information security risks management. The first essay emphasizes on how enterprises should set up internal strategies such as compensation strategies and authority delegation for ensuring information security. Since information security is not just about technology but it is about business process with real organizational involvement, it is important for enterprises to appropriately align finance and human resources with their security policy and practices for information assets. The second essay formally investigates how a firm's information security and privacy practices influence customer perception, satisfaction and financial performance. More importantly, this study can give firms insights into how to set up their practices for customer willingness to invest in a long-term business relationship by providing personal information.

The remainder of the dissertation is organized as follows. Chapter 2 proposes the first essay to examine the relationship between information security risk management and IT executive structural status in a Top Management Team. The theoretical framework and results are discussed in the subsections. Chapter 3 presents the second essay where we discuss the effects of information security and privacy practices on customer perceptions, firms' actual performance, and customer satisfaction. Chapter 4 concludes the proposal.

Chapter 2 . Information Security Management and IT Executives in a Top Management Team

2.1 Introduction

As information assets have become a critical factor for enterprises to stay competitive, there is an increasing awareness of information security, which ensures confidentiality, integrity and availability of information, as a strategic issue for many enterprises. Furthermore, legislative compliance requirements such as the Sarbanes-Oxley (SOX) have made information security more critical as an integral factor for good corporate governance by mandating stricter control over information (ITGI, 2006). One of the most significant provisions of the SOX is Section 404 which requires public companies to include an assessment report of the effectiveness of internal controls over financial procedures, including IT controls as well as to publicly provide the information for shareholders. By establishing and documenting internal controls, companies can attest to the validity and integrity of financial information from the time such information enters the company to the completion of the annual report each year. The SEC also requires that each company's external auditors independently review management's assessment of internal controls and document any material weaknesses the audit firm discovers. The evaluation of internal controls includes not just about the quality of accounting or financial information systems, but also about the quality of information security risk management (ISACA®, 2006). Gordon and Loeb (2006) provided empirical evidence that SOX has made firms more cognizant of their information security activities. This fact implies that information security is more necessary than ever. Furthermore, the Public Company Accounting Oversight Board (PCAOB), established by the Sarbanes-Oxley Act,

mentioned that IT (Information Technology) internal control weaknesses should be considered as an enterprise level control, given the extensive and pervasive usage of IT in the enterprises' daily business processes and transactions. Basu et al. (2008) also claimed that risk management in information security governance is not simply a technical issue, since it requires an enterprise-wide dimension such as policies and standardization for reporting, roles, and accountability (Basu & Jarnagin, 2008).

Numerous researchers and practitioners have argued that successful risk management in information security governance can be achieved only through effective board oversight, since the board can control risks across an entire enterprise (Campbell, Gordon, Loeb, & Zhou, 2003; Gordon & Loeb, 2002; McFadzean, Ezingeard, & Birchall, 2007; Staw, 1980). Many enterprises have appointed high-level IT executives who are able to strategically and operationally conduct liaison activities between IT and other business units (Enns, Huff, & Higgins, 2003; Mitchell, 2006; Preston, Chen, & Leidner, 2008; Stephens, Ledbetter, Mitra, & Ford, 1992a; Stephens, Ledbetter, Mitra, & Ford, 1992b). The IT executive-level professionals such as the CIO (Chief Information Officer), CTO (Chief Technology Officer), CSO (Chief Security Officer), and CISO (Chief Information Security Officer) have been key figures responsible for governing and securing IT (Gartner, 2008).

However, despite the increased emphasis in executive level leadership for risk management in information security governance, few empirical studies have focused on the structural status of IT executives and their involvement in a Top Management Team (TMT) (Santalo & Kock, 2009; Smaltz, Sambamurthy, & Agarwal, 2004; Yayla & Hu,

2008). A lack of IT executive strategic decision-making authority prevents IT executives from acquiring peer acceptance and prevents their performance as a liaison between IT and non-IT units (Preston et al., 2008). Given the cross-functional role of IT executives for ensuring enterprise-wide information security, we argue that IT executives need to be deeply involved in a TMT and fairly compensated in order to lead strategic information security initiatives. Since many enterprises consider information an important asset, information security and controls have become the common denominator in areas of risk addressed by corporate governance standards including strategic, financial, technical, operational, and regulatory risks. As a result, IT executive leadership with fair compensation and membership in a TMT has become a key ingredient in any successful strategic information security initiative (Johnston & Hale, 2009; Raghupathi, 2007).

Therefore, understanding the relationship between IT executives' structural status in a TMT and information security management, helps an enterprise successfully set strategies for executives to delegate authority and responsibility for ensuring the security of information assets. Previous research mainly focused on the technical characteristics of information systems risks such as software design, databases, and systems architecture and hardware performance (Cavusoglu, Mishra, & Raghunathan, 2005; Muralidhar, Parsa, & Sarathy, 1999; Posthumus & von Solms, 2005; Straub & Welke, 1998). Instead, our managerial approach allows the study to integrate these IT issues into a social context which takes into account the enterprise's norms for information security and IT internal controls. Also, our interdisciplinary study across behavioral economics, accounting, finance and information systems may be a beneficial way of exploring the wider issues of

information systems risks. With this purpose, we derived the primary research questions as following: *Does IT executives' involvement in a TMT have any relationship with achieving better risk management of information systems? Does IT executive authority and motivation created by fair compensation effectively govern a firm's information security?* In addition, we investigate how an enterprises risk management performance can be affected by IT executive turnover as a proxy of IT strategy continuity as well as pay dispersion between IT and non-IT executives.

The paper is structured in five main sections. In the next section, we review prior literature and then provide the research model and theoretical support for the hypotheses in Section 3. The methodology section describes the data collection process, the measures, and presents the descriptive statistics. Then, we follow with a presentation of our empirical analysis results. Finally, the paper discusses the results and the implications for future IT research and management practice.

2.2 Literature Review

The SOX is one of the most important pieces of legislation affecting public US enterprises. Section 404 of the SOX addresses the necessity for IT internal controls over enterprises reporting and information systems. When applied to technology, this implies that information must be accurately recorded and shared in appropriate ways as well as that it must be secured from threats of unauthorized access, inappropriate changes and data corruption. Therefore, Information technology departments, internal and external audit teams, and other management departments must develop a working relationship to ensure these controls are deployed across all required functions. Enterprises should

validate the information they disclose by certifying internal controls adequately, and they also assure confidentiality, integrity, and availability of the data from IT-related risks such as information system disasters, electronic fraud, cyber-attacks, and identity theft (SEC, 2005). The required assessments are forcing many enterprises to identify and resolve IT internal control deficiencies (Smith, 2004; Wendell, 2005). It has become readily apparent that IT internal controls and information security, under the umbrella of IT governance, must align with corporate strategy to achieve reliable financial reporting, in order to meet SOX requirements. Furthermore, increased information breach incidents and electronic frauds have driven stricter legal requirements with Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPPA) and the USA Patriot Act (Turban, 2008). Accordingly, IT executives are increasingly supposed to provide stewardship for their enterprises in terms of IT internal controls and secured systems.

Therefore, in order to investigate the impact of IT executives' structural status in a TMT on information security management, we developed our research model three streams of literature. First, we employ accounting literature which emphasizes the link between the delegation of authority and responsibility and compensation choices in a firm (Nagar, 2002). Hall and Liedtka (2005) examined how executives' compensation influences their strategic decisions for large-scale outsourcing. They considered a firm's compensation strategy as the ex ante effect on its performance and then demonstrated that the authority and motivation created by compensation significantly influence large-scale IT decisions (Hall & Liedtka, 2005). Yayla and Hu (2008) investigated the impacts of IT

executive compensation on firm performance with agency theory. Their results showed that the IT and non-IT compensation alignment is closely related to firm performance. As the ex ante effect of compensation on firm performance like prior literature, our paper examines IT executive compensation levels in a TMT as a proxy of authority or influence for strategic decision making on IT internal controls and security.

Second, we incorporated the research which explains how pay dispersion among members in a team affect enterprise performance. Prior literature demonstrated pay dispersion not only reflects the structural status, but may impair executive collaboration by creating perceptual and substantive barriers (Eisenhardt & Bourgeois, 1988; Miles & Snow, 1978). Henderson and Fredickson (2001) suggested that because more equal compensation promotes collaboration, greater coordination needs encourage smaller compensation gaps. Thus the combination of greater needs and smaller gaps enhances enterprise performance. According to this research, we argue that considering IT executives' liaison activities between IT and other business units, pay dispersion among IT units and other units can represent the IT executives' structural status, authority, and accountability.

Third, we examine the impact of IT strategy continuity by measuring IT executive turnover. Lower rates of turnover result in better performance because turnover might provide discontinuity in an enterprise's operation and strategy; as well as increase indirect costs (Huselid, 1995). Kesner and Sebora (1994) claimed that frequent senior executive turnover may disrupt organizational continuity and hurt enterprise performance (Kesner & Sebora, 1994). Therefore, we also investigated the impact of IT executive

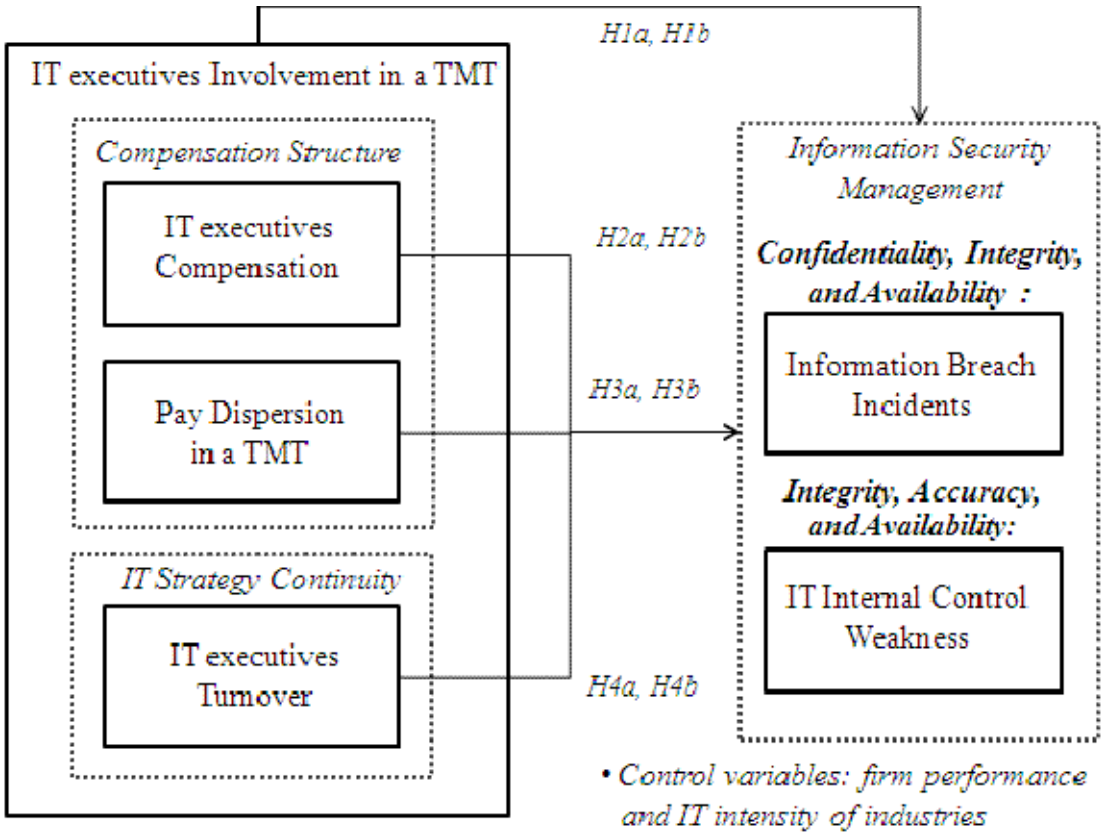
turnover on IT internal controls and security at the organizational level in terms of IT strategy continuity.

2.3 Conceptual Model and Research Hypothesis

As a part of IT governance, IT internal controls and information security are assigned to risk management which addresses the safeguarding of information assets, disaster recovery and continuity of operation. The Public Company Accounting Oversight Board (PCAOB) released guidelines for auditors that discuss IT internal controls in March 2004. It is necessary for companies to review their systems and applications for Data Security and Access Controls, Integrity and Accuracy of Data, Reliable Reporting Systems, and Disaster Recovery. Furthermore, companies need to demonstrate characteristics such as transparency, responsibility, and accountability, in order to gain the trust and support of the community or markets that they service. Information security has become a business priority that demands the attention of corporate boards and executive management. Thus, companies should be aware that the final responsibility for information security risk management rests with delegating fair authority to executive management as well as making sure the constraints of that delegation are communicated and clearly understood (ITGI, 2006). Information security management definitely requires, as stated previously, collaboration among IT, non-IT units, and internal and external teams for IT internal controls and security over enterprise systems. IT executives take responsibility of conducting liaison activities among them (Preston et al., 2008; SEC, 2005). Next, we developed the research model by integrating information security management with behavioral economics. The goals of information security have held confidentiality,

integrity and availability (known as the CIA triad) as the core principles of information security. Information security management is the process of carrying out various activities that achieve the goals of information security.

Figure 2.1 Research Model



As the measures of a firm's level in information security management, this study employed information security breach incidents and IT internal control weaknesses. First, information security breach incidents reflect a firm's confidentiality which is the ability of preventing disclosure of information to unauthorized individuals or systems. Second, the assessment of internal controls report is designed to assure investors that a company has the necessary procedures and controls in place to adequately ensure the integrity and

validity of its information. Therefore, IT internal control weaknesses demonstrate a firm's level in integrity, accuracy, and availability of information assets and systems.

IT internal controls weaknesses and information breach incidents involve all internal as well as external information security issues. Based on various identified internal and external security requirements, Information security demands the attention of executive management and all employees need to be engaged in them in their day-to-day work. Thus, successful information security management can be achieved, only if top level executives give it their complete support and commitment. Figure 1 shows a graphical summary of our conceptual framework with the specific constructs to answer the research questions.

Enterprises started to appoint IT executives to effectively manage information assets in the early 1990s. These moves are reflective of changes in top management thinking and strategy regarding the cross-functional role of IT executives, who are responsible for the security, accuracy and the reliability of the systems that manage and report the information. IT executive membership in a TMT can be considered as an antecedent of their high-level structural status for strategic organizational decisions (Gartner, 2008). It leads to sound strategic alignment and execution in order to ensure enterprise-wide information security and IT internal controls. So, we hypothesize that

Hypothesis 1a: *The possibility of information security breaches is negatively associated with IT executives' involvement in a TMT.*

Hypothesis 1b: *Weaknesses in IT internal controls is negatively associated with IT executives' actual involvement in a TMT.*

Although it has been several years since the realization of the critical role of IT executives in TMTs, the simple presence of IT executives in TMTs does not indicate the presence of the authority for strategic risk management decisions. Hall and Liedtka (2005) provided the first evidence of a relationship between compensation structures and strategic decisions. Aggarwal and Samwick (2003) demonstrated that executives with broad oversight authority have higher compensation-performance sensitivity. Prior literature has commonly emphasized the positive influence of compensation on an individual's performance as well as enterprise performance (Aggarwal & Samwick, 2003; Carpenter & Sanders, 2002; Core, Holthausen, & Larcker, 1999; Hall & Liedtka, 2005). Based on this literature, we study the more specific relationship between IT executives and their performance on risk management. So, we propose our next set of hypotheses as:

Hypothesis 2a: *The possibility of information security breaches is negatively associated with IT executives' compensation level.*

Hypothesis 2b: *Weaknesses in IT internal controls is negatively associated with IT executives' compensation level.*

The issue of pay dispersion across managerial team members has received attention by organizational theorists. There has been considerable research examining the implications of two competing theoretical models: one dealing with pay dispersion-tournament and the other with equity fairness. Tournament theory suggests that a large pay dispersion provides strong motivation to highly qualified managers, leading to improved enterprise performance (Lazear & Rosen, 1981). On the other hand, equity fairness tells that greater pay dispersion increase dysfunctional behavior among team

members, adversely affecting enterprise performance (Pfeffer & Langton, 1993). Considering the emphasized importance of enterprise-wide collaboration on risk management, we argue that equity fairness theories more appropriately explain IT executives' performance as the liaison between IT and other business units. Therefore our next hypotheses are:

Hypothesis 3a: *The possibility of information security breaches is positively associated with pay dispersion between non-IT and IT executives.*

Hypothesis 3d: *Weaknesses in IT internal controls is positively associated with pay dispersion between non-IT and IT executives.*

While some research has suggested that executive turnover creates discontinuity in a firm's operations and strategies, recent research has reported it does not always have a negative effect. The conflicting views concerning the effects of turnover suggest that one must not view turnover as a monolithic concept, but rather as a contingent phenomenon (Ton & Huckman, 2008). From the unique perspective of IT executive turnover, Perlman (2007) shows the turnover of IT executives has been high compared to other executives. Frequent turnover could be disruptive to any agency, but it is particularly damaging to information security processes which encompass an entire organization and undergird so many governmental services (Perlman, 2007). Although the importance of IT executives has increased in organizations, their positions have continued to be one of the most politically dangerous and operationally difficult executive positions, since information technology is expensive, volatile, complex and politically risky and so they need to handle rapidly changing job responsibilities and

dynamic information requirements. For instance, the frequent turnover of IT executives might result in discontinuity in the organizational and structural operations IT systems as well as IT strategies for risk management. Therefore, IT executives' turnover attests the severe pressure that is now being placed on individuals at the top IT executive level within the firm. So our next hypotheses are:

Hypothesis 4a: *The possibility of information security breaches is positively associated with IT executives' turnover.*

Hypothesis 4b: *Weaknesses in IT internal controls is positively associated with IT executives' turnover.*

2.4 Data collection and Research Methodology

The empirical analysis of this study includes two dependent variables. One includes information security breach announcements by publicly traded U.S. firms. The other has a firm's IT internal control evaluation by external auditors. We collected information security breaches from *Leixs/Nexis*, *CNet, ZDNet,* and *www.IdentityTheft.info*, searching news wires for the key words "information security breaches, identify theft, hacking, site attack, virus, data theft, or privacy breaches". As Sarbanes-Oxley (SOX) was announced in 2002, internal controls and information security have been one of the most critical issues for public enterprises. Thus, we considered information breach incidents between 2003 and 2008. In this time frame, there have been 1,486 information security breaches announced. We eliminated information breaches from government/military, medical/healthcare, and educational institutions. Finally, 577 incidents from the business

sector were collected and 232 incidents among them come from publicly traded firms in S&P 1500.

Second, public companies' internal controls weaknesses were collected from the Audit Analytics in WRDS between 2004 and 2008. Section 404 of SOX requires all public companies to report on the effectiveness of internal control for fiscal years ending on or after 2004 as part of their annual filing with the SEC. The Audit Analytics is widely used by accounting researchers to capture management assessment of internal control effectiveness (Doyle, Ge, & McVay, 2005; Doyle, Ge, & McVay, 2007; Kim, Robles, Cho, Lee, & Kim, 2008; Li, Lim, & Wang, 2007; Stoel & Muhanna, 2009). According to the Audit Analytics' classification, we categorized the types of internal controls weaknesses into IT internal control weaknesses and non-IT control weaknesses. We only used the IT internal controls weakness data.

Third, we constructed our measures for executive compensation and turnover using the ExecuComp distributed by Standard and Poor's. The ExecuComp database contains all information on total compensation from the top five executives up to 9 executives at each of the firms in the S&P 1500, and it is used extensively for empirical research. The two main advantages of ExecuComp relative to other data that have been used to examine executive compensation are that it contains a wide cross-section of firms and that it contains data not only for CEOs but other executives as well. We identified that ExecuComp has 1,462 firms reported from 2002 to 2008. However, 283 firms have IT executives under several titles like chief technology officer, chief information officer, chief security officer, and chief information security officer. Our sample has 232

incidents in information breaches and 158 cases in IT internal controls weaknesses. We extracted controls from 1,462 firms from the ExecuComp database, and conducted case-control studies with breached firms and IT internal weakness, respectively. In addition, we use the Bureau of Economic Analysis (BEA) annual data for the period 2002-2007 in industries in the United States for the level of IT equipment investments in a firm. Based on these data sources, we constructed the measures for our empirical models as follows. Table 2.1 shows the definitions of all variables in the models.

Breaches (BREACH). Breaches of confidentiality take many forms. For example, if a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. A firm's information systems attempt to enforce confidentiality by encrypting sensitive information during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. Also, breaches of availability fail to prevent service disruptions due to hackers' vandalizing a web site or denial-of-service attacks. Lastly, breaches of integrity include malwares or computer virus. We examined whether information breach incidents occur at a year *t*. If a firm has at least one breach incident at time t, then *BREACH* equals to one, otherwise 0. Appendix A. lists all types of breaches publicly announced at between 2003 and 2008.

IT internal control weakness (ITCW). We collected IT internal controls weakness from Audit Analytics, which provides a consistent methodology for considering the types of internal control weaknesses. Evaluating internal controls means attesting to the validity

and integrity of information systems from the time information enters the company to the completion of the annual report each year. The SOX requires that each company's external auditors independently review management's assessment of internal controls. Among internal controls, non-IT internal controls weakness such as accounting and financial reasons were eliminated by coding as 0. Then IT internal controls weaknesses were included as an indicator variable which is set as 1.

IT Executives (ITEXT). The first variable was the involvement of IT executives in each company's Top Management Team. If a company has an IT executive at the previous year when an information breach incident occurred, the value equals 1. Otherwise, it equals to 0.

Total compensation (TDC). We defined each executive's compensation as the sum of short-term and long-term compensation because the inclusion of only the short-term components of salary and bonus substantially understates the value of an individual's total remuneration (Lambert et al. 1993). Short-term compensation included salary and bonus. Long-term compensation was valued as the sum of stock options, restricted stock, performance share awards, performance units/cash awards, and dividend equivalents. For controlling the difference of compensation based on a firm size, the total compensation of the model is divided by the number of employees as a firm size.

Pay Dispersion (DISPERSION). Pay Dispersion represents the disparity of short-term compensation at year *t-1*, when an information breach incident occurred at year *t*. We compared the standard deviation of non-IT executives with that of IT executives and their means of compensation.

Table 2.1 Variable Definitions

Variables		Value	Source	Description
BREACH	Information Security Breaches	1 or 0	*Leixs/Nexis, IdentityTheft.info, CNet,and ZDNet*	If firm *i* had information breach incidents during year *t*, otherwise 0.
ITCW	IT internal controls weakness	1 or 0	*Audit Analytics*	If firm *i* had IT internal controls weakness during year *t*, otherwise 0.
TDC	Total Compensation	Thousands	*ExecuComp*	Salary, Bonus , Stock/Options, and Others
ITEXT	IT Executives	1 or 0	*ExecuComp*	If firm *i* had an IT executive in its top 5 executives during year *t*, otherwise 0.
DISPERSION	Pay Dispersion	-	*ExecuComp*	The disparity of compensation between IT and non-IT executives in a TMT
TURNOVER	The turnover of an IT executive	The number of turnovers	*ExecuComp*	If firm *i* had the number of IT executives during the previous year.
ITINT	IT Intensity	-	*BEA*	Industry ITINT/FTE over Overall ITINT/FTE
FVALUE	Firm performance (ROA)	Thousands	*Compustat*	ROA for the fiscal year.

Notes. *BEA stands for Bureau of Economic Analysis. ITINT stands for IT equipment. FTE stands for Full-Time Employee*

Turnover (TURNOVER). We examine whether information breach incidents are more likely to occur if an IT executive departed at t-1. We included a binary variable that equals to one if an IT executive left in the period.

IT Intensity (ITINT). We use the ratio of IT capital to labor which has been generally employed by previous IS literature (Park, Shin, & Sanders, 2007; Zhu & Kraemer, 2002). From the BEA annual data for the period 2002-2007, we ranked all industries based on the intensity in their use of IT equipment, which includes computers and peripheral equipment, software, and other information processing equipment (Dumagan & Gill, 2002). We calculated the ratio between IT equipment per Full-Time Employee (FTE) for each industry and the average IT equipment per FTE for all industries. The IT intensity of an industry *i* is derived by the following equation. We need to control for various industry effects, because they lead to different interdependencies among TMT members (Siegel & Hambrick, 2005). In this study, IT intensity is controlled by employing a case-control study with firms that are in the same 2-digit Standard Industrial Classification (SIC) code and the nearest firm performance based on ROA

$$ITINT_{i,t} = \left(\frac{IT\ Equipment_{i,t}}{FTE_{i,t}}\right) / \left(\frac{IT\ Equipment_{total,t}}{FTE_{total,t}}\right)$$

Firm Performance (FVALUE). A firm's performance can influence both pay level (Ehrenberg and Smith, 2003) and the mix of different pay components (Zenger and Marshall, 2000). We also considered enterprise performance, which is positively associated with the relative importance of incentives (Anderson, Baker, Ravindran, 2000) by adding each firm's *ROA*, since more profitable enterprises may be able to pay more.

Table 2.2 provides the descriptive statistics for all samples. We used logistic regression analysis to test our hypotheses with the sample data.

Table 2.2 Descriptive Statistics

Variable	Mean	Std Error	Median	Minimum	Maximum
A. All firms from the industries which had at least one breach or weakness from 2002 to 2008, n=1,462					
IT intensity	2.66	0.134	1.27	0.110	22.98
ROA	6.661	0.783	5.705	-151.865	1,100
B. The firms with Information Security Breaches from 2003 to 2008 in t year, n=232					
IT intensity	2.408	0.289	0.840	0.100	22.98
ROA	3.863	0.456	3.663	-32.324	21.106
C. The firms with IT internal controls weaknesses from 2004 to 2008 in t year, n=158					
IT intensity	2.842	0.402	1.135	0.110	22.98
ROA	7.429	7.116	1.503	-151.865	1,100
D. The firms without IT executives(ITEXEC=0 in from 2002 to 2007) in t-1 year, n=1,169					
IT intensity	2.660	0.134	1.270	0.100	22.98
ROA	6.783	0.968	5.395	-151.856	1,100
E. The firms with IT executives (ITEXEC=1 in from 2002 to 2007) in t-1 year, n=283					
Compensation	777.919	19.458	738.019	2.252	2,343.364
Pay Dispersion	3.200	3.451	1.066	-298.99	292.187
Turnover	0.923	0.011	1	0.333	1
IT intensity	1.746	0.180	1.00	0.13	22.98
ROA	6.158	0.412	6.526	-47.645	18.114
F. The firms with breach incidents (BREACH=1 in t year and ITEXEC=1 in t-1 year), n=49					
Compensation	784.226	65.471	770.191	5.712	2,343.364
Pay Dispersion	3.217	19.650	0.066	-298.99	292.182
Turnover	0.939	0.025	1	0.5	1
IT intensity	1.377	0.119	1.59	0.64	2.1
ROA	5.672	1.005	5.05	-10.497	16.659
G. The firms with IT internal control weaknesses (ITCW=1 in t year and ITEXEC=1 in t-1 year), n=33					
Compensation	731.138	60.418	770.714	2.252	1,427.275
Pay Dispersion	4.466	3.242	1.170	-3.476	74.128
Turnover	0.917	0.036	1	0.5	1
IT intensity	1.17	0.195	0.74	0.17	3.72
ROA	-0.012	1.417	1.048	-15.908	10.643

A case-control study was conducted among firms which have information breaches, IT internal controls weaknesses or neither. For each of the case firms, we selected 3 control firms that were not charged with information breaches and IT internal control weaknesses, respectively. The control sample consists of the firm in the first 2-digit SIC code that were nearest in enterprise performance, as measured by ROA. Then, we first examined the main effects of IT executive engagement in a TMT. The model (1) tests Hypothesis H1a with the dependent variable, which represents the probability of having no breach. $BREACH_{it}$ equals to 0 if firm *i* does not have any information breach incident during year *t*. The sample includes both breached and non-breached firms.

$$Pr(BREACH_{i,t} = 1|x_{i,t-1}) = \alpha_0 + +\alpha_1 ITEXE_{i,t-1} + \gamma_1 FVALUE_{i,t-1} + \gamma_2 ITINT_{i,t-1} \quad (1)$$

In order to test H2a ~H4a with information breaches as a dependent variable, the model (2) was constructed. The model examines how a firm' compensation strategies and the TMT structure with IT executives influence the probability of that the firm has information breach incidents.

$$Pr(BREACH_{i,t} = 1|x_{i,t-1}) = \beta_0 + \beta_1 TDC_{i,t-1} + \beta_2 DISPERSION_{i,t-1} + \beta_3 TURNOVER_{i,t-1} + \gamma_3 FVALUE_{i,t-1} + \gamma_4 ITINT_{i,t-1} \quad (2)$$

Then, we developed the model (3) and (4) to test H1b~ H4b using SOX404 which represents a firm's IT internal controls weakness provided by external auditors. The model (3) tests the relationship between IT executive engagement in a TMT and IT internal controls weaknesses for H1b.

$$Pr(ITCW_{i,t} = 1|x_{i,t-1}) = \alpha_0 + \alpha_1 ITEXE_{i,t-1} + \gamma_1 FVALUE_{i,t-1} + \gamma_2 ITINT_{i,t-1} \quad (3)$$

The model (4) investigates the effects of compensation level, pay dispersion in a TMT, and the turnover of IT executives on IT internal controls weaknesses.

$$Pr(ITCW_{i,t} = 1|x_{i,t-1}) =$$

$$\beta_0 + \beta_1 TDC_{i,t-1} + \beta_2 DISPERSION_{i,t-1} + \beta_3 TURNOVER_{i,t-1} + \gamma_3 FVALUE_{i,t-1}$$

$$+\gamma_4 ITINT_{i,t-1} \quad (4)$$

Table 2.3 Correlation Matrix of the Variables and Tolerance Value

	ITCW	1	2	3	4	Tolerance	VIF
Breaches	-0.141** *(.0355)*						
1. Compensation		1.00				0.856	1.168
2. Pay Dispersion		-0.497*** *(<.0001)*	1.00			0.992	1.007
3. Turnover		0.236*** *(.0004)*	-0.301*** *(<.0001)*	1.00		0.849	1.177
4. Firm Performance		-0.0754 *(.2613)*	-0.0129 *(.8472)*	0.0459 *(.4936)*		0.914	1.094
5. IT Intensity		0.1549** *(.0204)*	-0.0402 *(.5497)*	-0.0737 *(.2723)*	-0.0708 *(.2912)*	0.932	1.073

*Notes. P-values are in parentheses. . * Significant at 10%, ** Significant at 5%, *** Significant at 1%.*

Table 2.3 displays the correlation matrix. The correlations among the independent variables show low values. We also conducted a formal multicollinearity test with the regression. The multicollinearity diagnostic returns a tolerance value of between 0.87 and 0.99, which is above the common cutoff threshold of 0.1 (Hair, Tatham, Anderson, & Black, 2005). The variance Inflations (VIFs) of all variables are less than 1.4. Thus, multicollinearity is not a concern for our models.

Table 2.4 Logistic Regression Results

	IT executive's involvement	Compensation			Hypotheses
		Short-term	Long-term	Total	
Probability (Breaches=1)					
Independent Variables					
IT Executives (α_1)	-0.3659* *(0.215)*				*H1a:Supported*
Compensation (β_1)		-2.863** *(0.927)*	-6.105** (2.367)	-4.987** (1.700)	*H2a:Supported*
Pay Dispersion (β_2)		-0.018*** *(0.006)*	-0.045** *(0.015)*	-0.035** *(0.015)*	*H3a:Supported*
Turnover (β_3)		-1.246 *(0.850)*	-0.275 *(0.550)*	-0.109 *(0.571)*	*H4a:Not Supported*
Control Variables					
Firm Performance (γ_1,γ_2)	-0.327** *(0.105)*	0.081 *0.266)*	0.198 *(0.276)*	0.022 *(0.291)*	
IT Intensity ($\gamma_3,\gamma_4,$)	-0.1471 *(0.097)*	-0.036 *0(.527)*	-0.115 *(0.301)*	-0.146 *(0.298)*	
Probability (IT Internal Control Weakness=1)					
Independent Variables					
IT Executives (α_1)	-0.725** *(.317)*				*H1b:Supported*
Compensation (β_1)		-4.366** *(2.232)*	-6.558** (2.761)	-7.140** (3.029)	*H2b:Supported*
Pay Dispersion (β_2)		-0.019** *(0.016)*	-4.471 *(3.346)*	-7.947* *(4.754)*	*H3b:・Supported in Total and Short-term ・Not supported in long-term*
Turnover (β_3)		1.528** *(0.733)*	0.810 *(0.617)*	2.77** (1.288)	*H4b:・Supported in Total and Short-term ・Not supported in long-term*
Control Variables					
Firm Performance (γ_1,γ_2)	-1.227*** *(0.140)*	-1.175 *(0.502)*	-0.209** *(0.074)*	-0.227** *(0.082)*	
IT Intensity ($\gamma_3,\gamma_4,$)	-0.254 *(0.109)*	-0.201 *(0.597)*	0.283 *(0.439)*	0.236 *(0.449)*	

Notes. *Standard errors are in parentheses. p-values are represented by * Significant at 10%, ** Significant at 5%, *** Significant at 1%. The models use an intercept term*

2.5 Results

Table 2.4 reports the results from our models. The results support five of the eights hypotheses, partially support two of them, and fail to provide the evidence for one hypothesis. First, we demonstrate that IT executive involvement ($ITEXT_{i,t-1}$) in a TMT is associated with a significant reduction in information security breaches and IT internal controls weaknesses as predicted. It indicates that when an IT executive is highly engaged in the TMT, there is a lower probability of information breach incidents. Also, we found IT executive's compensation level ($TDC_{i,t-1}$) is negatively associated with the possibilities of both information breaches and IT internal control weaknesses.

In terms of pay dispersion between non-IT and IT executives, its coefficient is significantly positive with the possibility of information breach incidents. However, the results partially support the effect of pay dispersion on IT internal control weaknesses. The pay dispersion of short-term and total compensation significantly decrease the possibility of IT internal control weaknesses, but that of long-term compensation doesn't have a significant effect on it.

For IT executive turnover, we fail to find evidence for its significant effects on information breach incidents, while the model shows partially significant effects on IT internal controls weaknesses in the models with short-term and total compensation variables. Interestingly, IT internal controls weaknesses have a positive relationship with an IT executive's turnover. Based on organizational studies literature, we can conclude the compound effect of turnover presents the conflicting views on enterprise performance for information security risk management.

2.6 Discussion and Conclusions

This paper provides the first comprehensive analysis of the impacts of IT executive structural status on information security risks management. The results represent several new insights. First, IT executive involvement in a TMT results in effective risk management of information security breaches and internal controls. Next, it implies IT executive high engagement in a TMT helps an enterprise successfully govern information security risks with initiatives for strategic alignment and execution (Preston et al., 2008). Second, IT executive's compensation positively affects ensuring information security. In addition, the pay dispersion between non-IT and IT executives has a negative effect on managing information security risks. Third, this study indicates IT executive turnover does not have a significant effect on information security. Our results may imply turnover has a compound effect, because it provides discontinuity on operation and strategy as well as the highest performance in the first year when an individual joins a firm (Staw, 1980). As one of the limitations in our study, IT executive's reporting relationship might be one of the significant factors in organizations, because it can add strength to the position of any IT executives who are attempting to convince management that they should report to a president rather than a controller or other executive. However, rather than measuring reporting relationships, our study has focused on the compensation structures which represent an inter-relationship among top executives rather than a hierarchical relationship. Our study provides enterprises with a benchmark for compensation strategies that can be helpful to assess information system risk management performance. Enterprises can use our findings to assess the merits of

acquiring IT executives with high authority and quality. The results also suggest IT executives with enough strategic decision-making authority and peer acceptance in organization cultural practices are positively associated with protecting information systems.

Chapter 3 . Consumer Privacy Concerns with Internet Service Types, the types of Information requested, and Consumer Characteristics

3.1 Introduction

The growth of business-to-consumer (B-to-C) electronic market has become phenomenal because the Internet has presented a new framework for engaging in B-to-C relationships and has emerged as an important marketing medium and channel. Thanks to the Internet it has been possible to map consumer behavior patterns and personal information (Bessen, 1993). Many firms have captured consumers' needs and adopted them for marketing techniques. However, the excessive use of personal information hurts consumers in various ways, such as its unsolicited emails, credit card frauds or identity thefts. For instance, Sears faced a class-action lawsuit after making its consumers' purchase history of public via a business partner web site[1]. Also, in May 2008 Charter Communications, one of the nation's largest Internet service providers, announced enhanced service plans by installing software to map its Internet consumers' browsing behavior in order to sell ads tailored to consumers' interests. But, consumers immediately protested and the plan was cancelled[2]. While the B-to-C electronic market has grown, consumers' increased Internet privacy concerns have negatively influenced their commitment to form a relationship with a firm due to providing personal information (Eastlick, Lotz, & Warrington, 2006).

---

[1] See *http://www.infoworld.com/article/08/01/08/Sears-sued-over-privacy-breach_1.html*
[2] See *http://www.slate.com/id/2198119/*

As more and more consumers have become anxious about protecting their information, it has been critical to identify how privacy concerns affect consumer willingness to form B-to-C relationship over the Internet and which factors accelerate or alleviate consumer privacy concerns. Although market research companies claim the benefits of e-business are numerous for consumers as well as companies, many consumers use internet channels for seeking information and still make their actual purchase through traditional channels (Barua, Konana, Whinston, & Yin, 2001). Wang and Emurian (2005) demonstrated information privacy concerns build "a most formidable barrier to people engaging in e-commerce" (Wang & Emurian, 2005). Indeed, since the electronic market involves high uncertainty, limited legal protection, and numerous competitors with low switching costs, alleviating consumer privacy concerns is considered as a necessity for building trust and satisfaction in buyer-seller relationships on the Intenet. (Luo, 2002; Schlosser, White, & Lloyd, 2006; Selnes, 1998; Steenkamp & Geyskens, 2006). While utilizing collected personal information has become a necessity to meeting consumers' needs, it also lays a heavy burden on a firm to ensure adequate privacy protection (Bowie & Jamal, 2006). Therefore, it becomes more critical for the electronic market to resolve consumers' security and privacy concerns. Therefore, the purposes of this paper are to understand how consumer privacy concerns influence their willingness to provide personal information with various online service types and how individual differences, e.g. Knowledge and Internet experience, affect consumer privacy concerns. The results can give firms new insights into how they can identify specific

information practices for consumer behavioral intentions or willingness to provide personal information for online B-to-C relationship.

We first synthesize literature of relationship marketing in B-to-C electronic commerce, and information privacy. Then, we propose a research model and report the results of the empirical analysis. Lastly, we discuss the implications of the results for practice and theory.

3.2 Literature Review

Information privacy issues have attracted researchers and there is a significant body of related research. Some previous research investigated the causes of privacy concerns (Milne & Boza, 1998; Petrison & Wang, 1993; Phelps, Nowak, & Ferrell, 2000; Sheehan & Hoy, 1999). This stream of research primarily contributes a better understanding of the factors that underlie privacy concerns and the ways in how policy and practices can be employed to reduce consumer concerns. Milne and Boza (1998) presented a model of the antecedents of concern and trust. Among the variables tested, their findings indicate that trust and perceived information control are negatively related to concern, while attitude toward a buyer-seller relationship in direct marketing is positively related to trust. Phelps et al. (2000) presented a conceptual model in which consumers' privacy concerns are determined by the type of personal information requested, the amount of information control offered, the potential consequences and benefits offered in the exchange, and consumer characteristics. They proposed these factors not only influence overall concern, but also influence consumer beliefs regarding marketers' information practices and that the outcomes of overall concern and beliefs influence consumers' future behavioral and

attitudinal responses. Our paper is different from their study in that it differentiate between the types of information requested over the Internet (e.g., financial versus demographics) and online service types (e.g., Search engines versus Online retailers), while Phelps et al. (2000) and Milne et al. (1999) focused on consumers' purchase decisions upon privacy concerns in interacting with direct marketers. Based on the relationship between privacy concerns and consumer characteristics, this study also involves consumer individual differences (i.e., Internet usage and experiences with information misuse).

Another stream of recent information privacy research is the examination of the consequences of consumer privacy concerns. Understanding the attitudinal and behavioral reactions that stem from privacy concerns is as important as understanding the antecedents (Phelps, D'Souza, & Nowak, 2001). Without a sense of the consequences, it is impossible to understand how important privacy concerns are for firms and consumers. This is especially important to the potential consequences of privacy concerns and related factors on establishing a long-term relationship, or purchase behavior. Sheehan and Hoy (1999) reported privacy concern makes respondents more likely to provide incomplete information to a website and request removal from mailing lists. Furthermore, as privacy concern increases, respondents were less likely to register at websites that request information. Many researchers demonstrated that consumers are reluctant to provide their personal information or participate in online transactions due to consumers' privacy concerns in a firm's obligations on both transactions and operations (Sipior, Ward, & Rongione, 2003). Internet privacy concerns can result in their willingness, or non-

willingness, to participate in the electronic market and disclose consumers' personal information (Ba & Pavlou, 2002; Lee & Turban, 2000; Suh & Han, 2003). If consumers cannot believe their transactions and data are handled safely and securely, they try to switch providers. In particular, the more competitive industry becomes, the more information firms require with various purposes such as personalized services or direct marketing. However, it can make consumers feel private information has been violated, while a firm believes it provides better services to consumers. The prior research has mainly focused on how privacy concerns negatively affect consumer purchase intention. Our study more specifically examines consumer willingness to provide different types of personal information based upon the types of firms' Online Services and Consumer Characteristics.

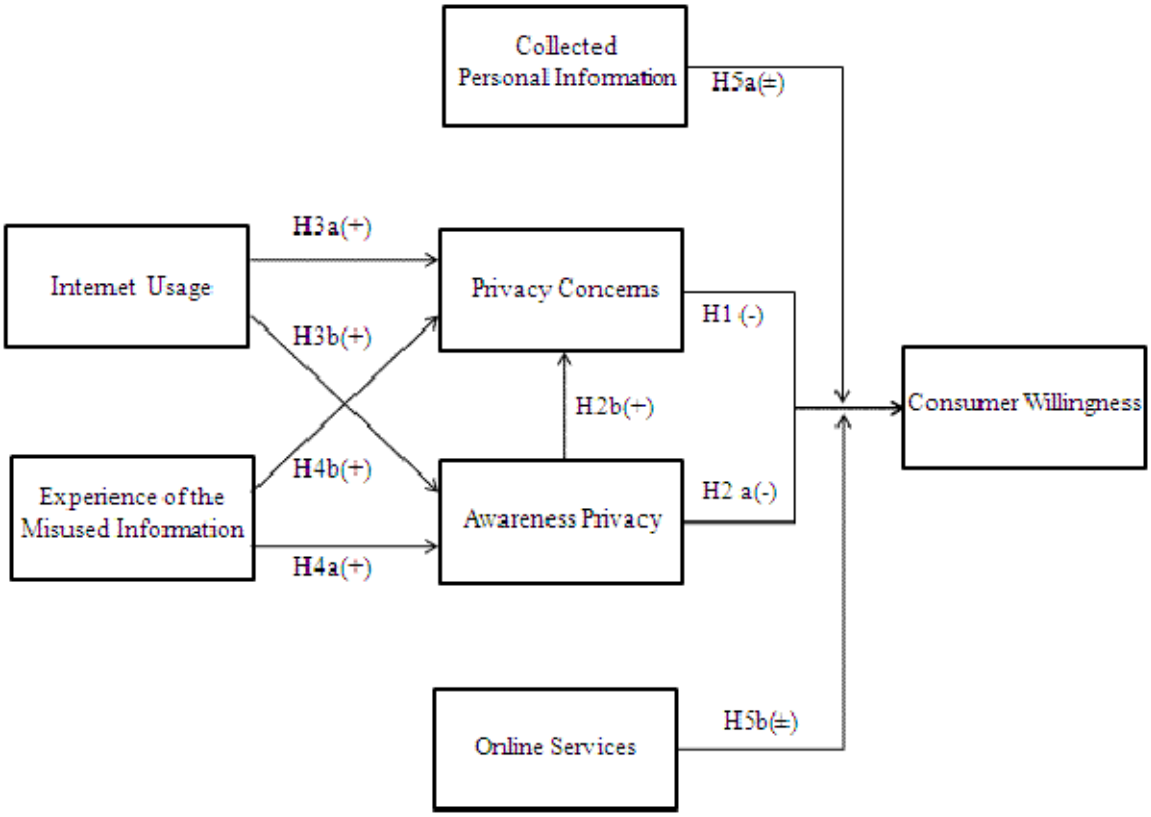
3.3 Research Methodology

Figure 3.1 shows the conceptual model. Most buyer-seller relationships are characterized by risks due to information asymmetry to the sellers' advantage (Mishra, Heide, & Cort, 1998). Pavlou and Gefen (2004) defined buyers' perceived risk from the community of sellers as buyers' perception that there is some probability of suffering a loss when pursuing transactions among members of the community of sellers in the specific marketplace. This study narrowly focuses on consumers' concern on information privacy among possible damages.

Consumer privacy concerns about the usage of their personal information required by a firm impact their behavioral intention to establish a relationship by providing personal information (Sheehan and Hoy, 1999). The behavioral intention for providing personal

information in establishing a relationship, can be defined as "Commitment toward a firm" (Morgan & Hunt, 1994). We employ The Commitment-Trust Theory to explain the relationship between consumer behavioral intention and firm practices for relationship marketing. Morgan and Hunt (1994) theorized that establishing successful long-term relations require commitment and trust (Morgan & Hunt, 1994). The Commitment-Trust Theory can provide theoretical guidance for examining consumer privacy concerns in B2C relationships.

Figure 3.1 The Proposed Conceptual Model and Hypotheses



Consumer personal information is increasingly viewed by firms as an important information asset used to deliver competitive advantage and support consumer-focused business initiatives. Consistent with the Commitment-Trust Theory, it can be predicted

that consumer concerns in a firm's obligation for privacy directly influence their commitment toward the firm. So, the study proposes the set of hypotheses as:

H1: *Consumer privacy concerns decrease consumer willingness to providing personal information with a firm over the Internet.*

Prior literature explains knowledge increase awareness of risks and it is essential for changes in behavior (Saavedra, 1996; Straub & Welke, 1998). Consumer privacy awareness might evoke their concerns about them. Firms have adopted technologies and fulfilled social and cultural requirements such as notification and consent in order to convince consumers of their fulfillment on privacy and security(Smith, Milburg, & Burke, 1996). The more knowledge consumers have about a firm's practices such as collecting data and use of personal information, the more concerned they may be about information privacy (Campbell, 1997). According to Dinev and Hart (2006), individuals with high privacy social awareness will in general closely follow privacy issues; the possible consequences of a loss of privacy due to accidental, malicious, or intentional leakage of personal information and the development of privacy policies (Dinev et al., 2006). Privacy awareness can be considered as an antecedent to the personal disposition to value privacy and security. Thus, we examine how consumer awareness in technologies, notification, and consent influence consumer privacy concerns. This hypothesizes:

H2a*: Consumer privacy awareness decreases consumer willingness to providing personal information with a firm over the Internet.*

H2b*: Consumer privacy awareness increases consumer privacy concerns.*

As the factors of the attitudes of individuals about information privacy, the paper includes consumers' Internet usage and the experience on the misused information (Campbell, 1997). First, Internet usage leads to different levels of privacy awareness, because Internet-usage can make consumers more exposed to Internet privacy risks (Luo, 2002; Miyazaki & Fernandez, 2000). Although the Internet brings us great websites full of information and entertainment, and email and chat have revolutionized communication, Internet users are increasingly concerned about how much of their personal information they are giving up in exchange. Comparing privacy concerns between light and heavy Internet users can show how consumers' concerns about privacy of personal information are changing as Internet use increases. Therefore, the hypotheses are:

***H3a**: Consumer Internet usage is positively associated with consumer privacy concerns.*

***H3b**: Consumer Internet usage is positively associated with consumer privacy awareness.*

When exploring privacy issues relating to individual consumer differences, personal experiences are one important factors (Smith et al., 1996). A fundamental principle of social psychology is that one trusts one's own experiences the most (Deutsch, 1962). Personal negative experience with the information misuse by a particular firm is likely to increase all aspects of consumer privacy concerns, since such experiences hurt consumers' trust in all firms' obligation in privacy and security (Campbell, 1997). Thus, personal negative experience with the misuse of information is anticipated to affect consumers' information privacy concerns.

H4a: *Consumer experience of the misused personal information is positively associated with consumer privacy concerns.*

H4b*: Consumer experience of the misused personal information is positively associated with consumer privacy awareness.*

We examine how the relevance of the information requested by a firm, influences consumer privacy concerns based on different online services. The relevance of the required information might be a more central factor affecting consumers' perception in a firm's intention to use their personal information (Phelps et al., 2000). For instance, if search engines such as Google or Yahoo require financial information, a user might doubt a firm's intention based on the relevance of the required information against its original functions. Thus, the following hypotheses are proposed:

H5a*: The types of information requested by a firm moderate the impact of consumer privacy concerns on consumer willingness to provide personal information.*

H5b*: The types of online services provided by a firm moderate the impact of consumer privacy concerns on consumer willingness to provide personal information.*

3.4 Data Analysis and Results

Internet survey was conducted from March, 2009 to May, 2009. Compared with the postal mail or telephone surveys, internet survey is a faster and cheaper way to collect a great amount of data. The written questionnaire contained three of the endogenous constructs including privacy concerns, consumer willingness to providing personal information over the Internet, and privacy awareness. They were assessed using a 5-point Likert scale. Items were adapted from past research privacy concerns (Eastlick et al.,

2006; Milne & Boza, 1998). Internet usage and experience of the misuse of personal information were added as single-item instruments. The total number of responses was 685, of which 615 were valid. Table 3.1 provides a summary of respondent characteristics.

Table 3.1 Demographic characteristics of respondents

	# of respondents		# of respondents
Income:	n=618	**Education:**	n=665
Less than $15,000	50	High school degree	211
$15,000 to under $25,000	61	Some college	251
$25,000 to under $35,000	78	College degree	150
$35,000 to under $50,000	109	Graduate school or degree	53
$50,000 to under $75,000	161		
$75,000 to under $100,000	73	**Marital Status:**	n=685
More than $100,000	86	Married	447
		Never Married	110
Age:	n=677	Widowed/divorced	128
18 to 24	24		
25 to 34	87	**Location of Residence:**	n=656
35 to 44	232	Urban	144
45 to 54	240	Suburban	317
55 and others	94	Rural	195
		Gender:	n=666
Employ Status:	n=673	Female	530
Full time	272	Male	136
Part time	115	**Ethnicity:**	n=661
Others	286	Caucasian	546
		Other	115

Consumer Willingness to provide personal information. Various types of firms collect and utilize specific consumer information to acquire competitive advantages in the tough market. Consumer personal information, requested by a firm, can be generally classified as contact, behavioral, demographic, and financial information (Meinert, Peterson, Criswell, & Crossland, 2006). The types of personal information have various degrees to

which each type draws consumer privacy concerns (Milne 1997; Nowak and Phelps, 1992). Table 3.1 lists the types and items that each type includes. This study measured consumer willingness for each type of information requested by different online services.

Table 3.2 The type of personal information requested by a firm

Categories	The Required Information
Contact Information	Name, E-mail address, Mailing address, Telephone numbers
Demographic	Gender, Age, Education, Income, Personal interests, Hobbies
Behavioral Information	Browsing habits
Financial Information	Credit card numbers, Bank account

Privacy Concerns. A five- item scale was designed to evaluate consumers' privacy concerns about firms' obligation and how they value privacy (Eastlick et al., 2006; Milne & Boza, 1998). Previous research on consumer privacy concerns can be divided into two sets of variables: contextual issues relating to the type of information and the organization collecting the data. Individual difference between consumers evoke various levels of privacy concerns (Campbell, 1997). A consumer's disposition to value privacy is shown to be an important predictor of perceived privacy risk. Furthermore, this essay examines how a firm's privacy assurance intervention through privacy policy could increase individuals' perceived privacy concerns and mitigate their privacy risk perceptions across the types of online services and information requested by a firm.

Privacy Awareness. Privacy awareness reflects the extent to which a customer is informed about privacy practices and policies, and third-party institutional mechanisms such as TRUSTe, BBB Online, WebTrust, and PWC Privacy (Olivero & Lunt, 2004). A three-item scale was employed to assess consumer privacy awareness.

Table 3.3 Measurement model results

Construct Indicator	Statement	Factor loading	Reliability
Willingness to provide personal information			0.830
	Willingness to provide Contact information (x1)	0.817	
	Willingness to provide Demographic information(x2)	0.782	
	Willingness to provide Browsing habits(x3)	0.838	
	Willingness to provide Financial information(x4)	0.765	
Privacy Concerns			0.703
	Concerns about firms' intention in collecting personal information (x5)	0.512	
	Concerns about firms' fulfillment in privacy statements (x6)	0.633	
	Rating the importance of privacy against personalized services(x7)	0.521	
	Rating the risk of usage of the requested information (x8)	0.530	
	Rating the risk of usage of the web behavior tracked(x9)	0.606	
Privacy Awareness			0.762
	Awareness about third-party institutional mechanisms(x10)	0.740	
	Awareness about privacy statements(x11)	0.707	
	Awareness about cookies(x12)	0.633	
Internet Usage			
	How many hours do you use websites per week? (x13)	–	–
Experience of the misused information			
	How many times have you encountered personal information misuse? (x14)	–	–

Online Services. This study categorized online services into two categories: Search engines and Online Retailers. This measure examines how the inherent functions of a website influence consumer willingness to provide each type of personal information

(Bart, Shankar, Sultan, & Urban, 2005; Phelps et al., 2000). To eliminate brand reputation, the survey gave specific examples which include Google and Yahoo for Search engines and Amazon.com for Online Retailers.

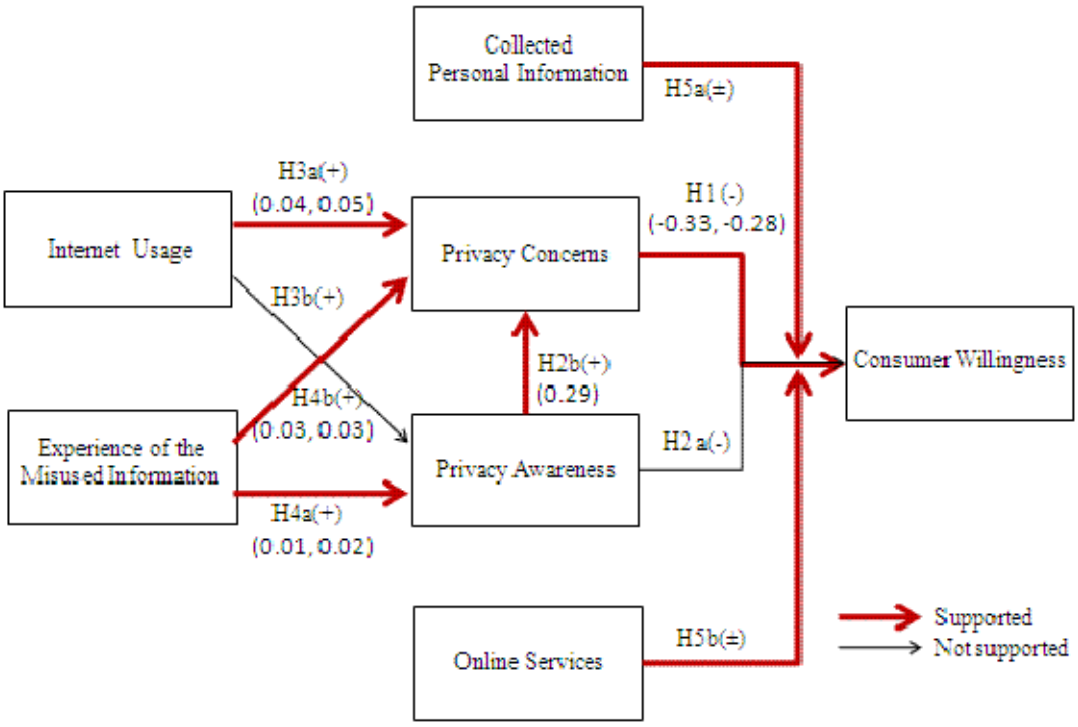
Table 3.4 Structural Model results

Path	Search Engines	Online Retailers
Privacy Concerns → Willingness to provide all personal information	-0.33*** (0.060)	-0.28*** (0.062)
Privacy Concerns →Contact/Demographic Information	-0.33*** (0.063)	-0.23*** (0.061)
Privacy Concerns →Behavioral Information	-0.36*** (0.065)	-0.29*** (0.063)
Privacy Concerns →Financial Information	-0.38*** (0.064)	-0.31*** (0.063)
Privacy Awareness → Willingness to provide all personal information	0.043** (0.021)	-0.014 (0.024)
Privacy Awareness → Privacy Concerns	0.29*** (0.042)	0.29*** (0.042)
Experience of the misuse → Privacy Concerns	0.031** (0.012)	0.033** (0.012)
Internet usage → Privacy Concerns	0.040*** (0.021)	0.050** (0.051)
Internet usage → Privacy Awareness	0.070 (0.049)	0.062 (0.049)
Experience of the misuse → Privacy Awareness	0.014*** (0.027)	0.027*** (0.027)
Model Results:		
Goodness of Fit Index (GFI)	0.95	0.94
Adjusted Goodness of Fit Index (AGFI)	0.92	0.91
Comparative Fit Index (CFI)	0.93	0.94
Root Mean Square Error of Approximation (RMSEA)	0.07	0.07

Tests of hypothesis. Structural equation modeling was conducted via LISREL 8.7 by employing the covariance matrix to estimate the structural model. The research model,

shown in Figure 1, consisted of exogenous and three endogenous constructs. Internet usage and experience of the misused information were used as single-item instruments. Prior to testing the structural model, principal component factor analysis was employed to test the construct reliability and validity. The results are presented in Table 2. The results provide evidence that the indicators and their underlying constructs were acceptable. Confirmatory factor analysis examines all multi-item scale (i.e., Willingness to provide personal information, Privacy and Security Concerns, and Privacy Awareness).

Figure 3.2 The Results of SEM Analysis



Results from structural equation modeling revealed good model fit as the GFI (0.94~0.95), AGFI (0.91~0.92), and CFI (0.93~0.94). Table 3 presents the model and structural path coefficients for each relationship. The latent variables were linearly determined by a set of observable exogenous causes and linearly determined a set of

observable endogenous indicators. This study employed multivariate analysis for examining the effect of two types of online services which include search engines (i.e., Google and Yahoo) and online retailers (i.e., Amazon.com). In addition, the study investigated how a consumer's willingness varies due to the required information, which search engines and online retailers required. The predicted negative relationships between consumer privacy concerns and consumer willingness (H1a) were supported with a coefficient, -0.33 ($p \leq 0.01$) and -0.28 ($p \leq 0.01$) in search engines and online retailers, respectively. This result shows consumers using search engines are more sensitive than those using the online retailer directly. It implies that privacy-sensitive consumers use internet channels for seeking information and still make an actual purchase through traditional channels, and that less privacy sensitive consumers prefer internet channels due to convenience. Furthermore, consumers' concerns have bigger effects on providing financial information (0.36 and 0.29) rather than contact information (0.33 and 0.23), respectively (H1c and H1d). The irrelevance of the financial information by search engines increases the effect of privacy and security concerns. The effect of consumers' knowledge in privacy and security on consumers' willingness is significant as 0.043($p \leq 0.05$) in search engines, while it is not significant in online retailers as -0.014 (H1b). However, consumers' knowledge in privacy and security positively impact their privacy concerns 0.29 ($p \leq 0.01$) in both of the online services (H2a). The experience of misused information is positively related to both privacy concerns and consumers' knowledge in privacy and security (H2b and H3b). While Internet usage also have

positive effect on privacy concerns, the model failed to show the evidence the effect of Internet usage on consumers' knowledge in privacy and security (H2c and H3a).

3.5 Conclusions

This study empirically examines how consumer privacy concerns influence their behavioral intention for providing personal information for a firm over the Internet. First, the paper synthesized information privacy concerns and relationship marketing literature, and then examined how the concerns influence online B-to-C relationship with various types of online firms. Second, the effects of consumer-related factors like knowledge and experience on Internet were considered. The results demonstrated that consumer privacy concerns negatively affect their behavioral intention to make a B-to-C relationship with a firm by making them reluctant to provide their personal information. Furthermore, this essay indicated that the levels of the impacts varies due to the Internet service types which firms offer as well as the types of the required information. While consumers' privacy concerns made them more reluctant to provide financial information for search engines than demographic information that implies a casual relationship. The results also showed that the types of the information required by firms influence consumer willingness to provide personal information by awaking their security and privacy concerns.

The privacy and security concerns more negatively affect their intentions to establish a relationship with online retailers than with simple information services. Lastly, the paper demonstrated the interrelationship among consumers' knowledge in privacy and security, experience of the misused information, and Internet usage, and security and

privacy concerns. These findings can give firms new insights into how they can set up their practices for acquiring consumer willingness to invest in a long-term business relationship.

Figure 3.3 Consumer Willingness with The types of Online services

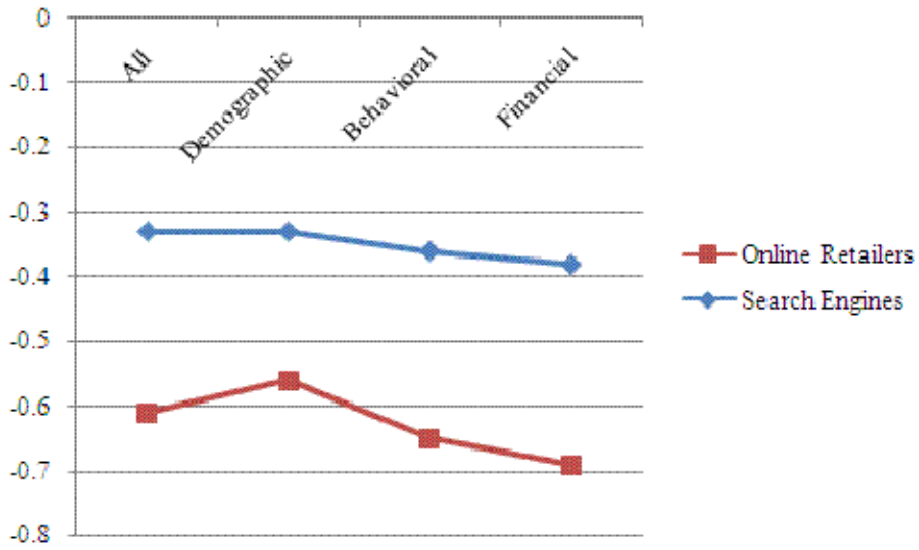
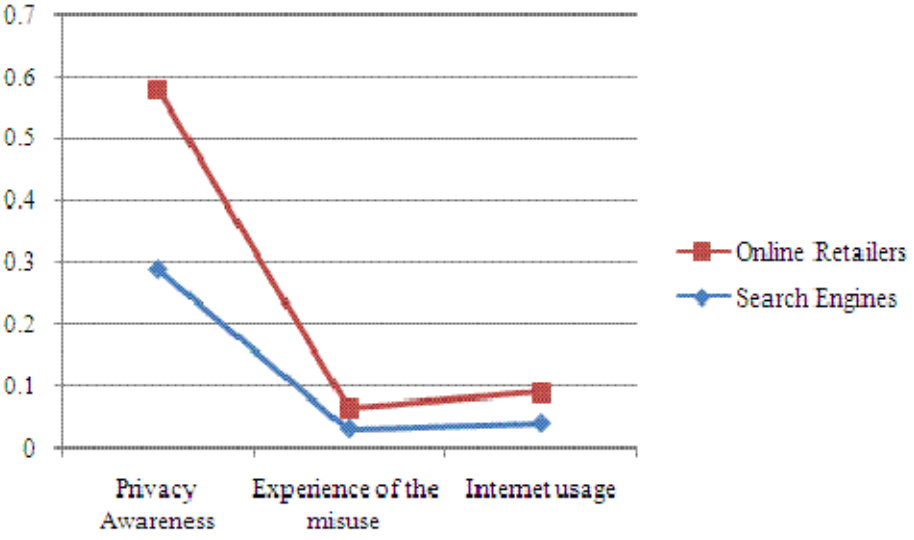


Figure 3.4 Privacy Concerns with Awareness, Experience, and Internet usage



In conclusion, this paper contributes to security and privacy issues in two major respects. First, the study provides substantive support for previous findings and additional

insights into the interrelationship among the concerns, behavioral intentions privacy, the types of online services, and consumers' other factors. Second, this paper sheds light in how a firm can resolve consumer privacy concerns based on its Internet service types and individual differences. For future research, we need to consider specific firms, their reputation, and brand image, since the direct and indirect effect of firm heterogeneity are strong influence on consumers' willingness. As the measures for this, the page view raking and brand equity can be considered. Further, future research could be undertaken to understand the multi-dimensions of consumer privacy concerns such as confidentiality, integrity, and availability, in order to clarify how each dimensions might related to established legal issue and potential differential effects of each on behavior.

Chapter 4 . Conclusions

This dissertation proposal provides two different perspectives in investigating information security management: compensation strategies for IT executives related to information breach incidents and IT internal control weaknesses, and information privacy strategies for enhancing consumer willingness to provide personal information with the types of online services and the types of information requested by each type of online service.

The first essay provides a comprehensive analysis to investigate the impacts of IT executive structural status on information security management. The results represent several new insights. First, IT executive involvement in a TMT results in effective risk management of information security breaches and IT internal controls. This fact implies IT executive high engagement in a TMT helps an enterprise successfully govern information security risks with initiatives for strategic alignment and execution (Preston et al., 2008). Second, IT executive compensation positively affects ensuring information security. In addition, the pay dispersion between non-IT and IT executives has a negative effect on managing information security risks. Third, this study indicates IT executive turnover does not have a significant effect on information security. Our results may imply turnover has a compound effect, because it provides discontinuity on operation and strategy as well as the highest performance in the first year when an individual joins a firm (Staw, 1980). Our study provides enterprises with a benchmark for compensation strategies that can be helpful to assess information system risk management performance. Enterprises can use our findings to assess the merits of acquiring IT executives with high

authority and quality. The results also suggest IT executives with enough strategic decision-making authority and peer acceptance in organization cultural practices are positively associated with protecting information systems.

The second essay empirically investigates how a consumer's privacy concerns influence their behavioral intention for providing personal information to a firm over the Internet. First, the paper combined information privacy concerns and relationship marketing literature, and then examined how the concerns influence online B-to-C relationship with various types of online services. Second, the effects of consumer-related factors like knowledge and experience on the Internet were considered. The results demonstrated that consumer privacy concerns negatively affect their behavioral intention to make a B-to-C relationship with a firm, and also suggested the levels of the impacts vary due to the Internet service types which firms offer as well as the types of the required information. While consumers' privacy concerns made them more reluctant to provide financial information for search engines than demographic information that implies a casual relationship. The results also showed that the types of information required by firms influence the consumer's willingness to provide personal information by awaking their security and privacy concerns. The privacy concerns more negatively affect their intentions to establish a relationship with online retailers than with simple information services. Lastly, the paper demonstrated the interrelationship among the consumer's knowledge of privacy and security, experience of misused information, Internet usage, and security and privacy concerns. These findings give firms new insights into how they can set up their practices for acquiring consumer willingness to invest in a

long-term business relationship. The second essay provides substantive support for previous findings and additional insights into the interrelationship among the concerns, behavioral intentions privacy, the types of online services, and consumers' other factors.

References

Aggarwal, R. K., & Samwick, A. A. 2003. Performance incentives within firms: The effect of managerial responsibility. ***Journal of Finance***, 58(4): 1613-1649.

Ba, S. L., & Pavlou, P. A. 2002. Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. ***MIS Quarterly***, 26(3): 243-268.

Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. 2005. Are the drivers and role of online trust the same for all Web sites and consumers? A large-scale exploratory empirical study. ***Journal of Marketing***, 69(4): 133-152.

Barua, A., Konana, P., Whinston, A. B., & Yin, F. 2001. Driving E-business excellence. ***Mit Sloan Management Review***, 43(1): 36-+.

Basu, A., & Jarnagin, C. 2008. How to Tap IT's Hidden Potential, ***The Wall Street Journal.Com***: http://online.wsj.com/article/SB120467900166211989.html.

Bessen, J. 1993. RIDING THE MARKETING INFORMATION WAVE. ***Harvard Business Review***, 71(5): 150-160.

Bowie, N. E., & Jamal, K. 2006. Privacy rights on the Internet: Self-regulation or government regulation? ***Business Ethics Quarterly***, 16(3): 323-342.

Campbell, A. J. 1997. Relationship Marketing in Consumer Markets. ***Journal of Direct Marketing***, 11: 46-48.

Campbell, K., Gordon, L., Loeb, M., & Zhou, L. 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. ***Journal of Computer Security***, 11(3): 431.

Carpenter, M. A., & Sanders, W. G. 2002. Top management team compensation: The missing link between CEO pay and firm performance? ***Strategic Management Journal***, 23(4): 367-375.

Cavusoglu, H., Mishra, B., & Raghunathan, S. 2005. The value of intrusion detection systems in information technology security architecture. ***Information Systems Research***, 16(1): 28-46.

Core, J. E., Holthausen, R. W., & Larcker, D. F. 1999. Corporate governance, chief executive officer compensation, and firm performance. ***Journal of Financial Economics***, 51(3): 371-406.

Deutsch, M. (Ed.). 1962. ***Cooperation and Trust: Some Theoretical Notes***: Lincoln, NE: University of Nebraska Press.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. 2006. Privacy calculus model in e-commerce - a study of Italy and the United States. ***European Journal of Information Systems***, 15(4): 389-402.

Doyle, J., Ge, W., & McVay, S. 2005. ***Determinants of weaknesses in internal control over financial reporting***. Paper presented at the Conference on Corporate Governance - Financial Report, Internal Control and Auditing, Cambridge, MA.

Doyle, J. T., Ge, W., & McVay, S. 2007. Accruals quality and internal control over financial reporting. ***Accounting Review***, 82(5): 1141-1170.

Dumagan, J., & Gill, G. 2002. Industry-Level Effects of Information Technology Use on Productivity and Inflation, ***U.S. Department o fCommerce***. Washington DC.

Eastlick, M. A., Lotz, S. L., & Warrington, P. 2006. Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. ***Journal of Business Research***, 59(8): 877-886.

Eisenhardt, K. M., & Bourgeois, L. J. 1988. Politics Of Strategic Decision-Making In High-Velocity Environments - Toward A Midrange Theory. ***Academy of Management Journal***, 31(4): 737-770.

Enns, H. G., Huff, S. L., & Higgins, C. A. 2003. CIO lateral influence behaviors: Gaining peers' commitment to strategic information systems. ***MIS Quarterly***, 27(1): 155-176.

Ernst, & Young. 2008. Moving Beyound compliance, Global Information Security Survey.

Gartner. 2008. The evolving role of CISO in the New security Order.

Gordon, L., & Loeb, M. 2002. The Economics of Information Security Investment. ***ACM Transactions On Information and System Security***, 5(4): 438.

Hair, J. F., Tatham, R. L., Anderson, R. E., & Black, W. 2005. ***Multivariate Data Analysis*** (6 edition ed.): Prentice Hall.

Hall, J. A., & Liedtka, S. L. 2005. Financial performance, CEO compensation, and large-scale information technology Outsourcing decisions. ***Journal of Management Information Systems***, 22(1): 193-221.

Huselid, M. A. 1995. The Impact Of Human-Resource Management-Practices On Turnover, Productivity, and Corporate Financial Performance. ***Academy of Management Journal***, 38(3): 635-672.

ISACA®. 2006. IT Control Objectives for Sarbanes-Oxley 2nd Edition: www.isaca.org/sox.

ITGI. 2006. IT Control Objectives For Sarbanes-Oxley: http://www.isaca.org/sox/.

Johnston, A. C., & Hale, R. 2009. Improved Security through Information Security Governance. ***Communications of the Acm***, 52(1): 126-129.

Kesner, I. F., & Sebora, T. C. 1994. Executive Succession - Past, Present and Future. ***Journal of Management***, 20(2): 327-372.

Kim, N. Y., Robles, R. J., Cho, S. E., Lee, Y. S., & Kim, T. H. 2008. SOX Act and IT Security Governance. ***International Symposium on Ubiquitous Multimedia Computing, Proceedings***: 218-221.

Lazear, E. P., & Rosen, S. 1981. Rank-Order Tournaments As Optimum Labor Contracts. ***Journal of Political Economy***, 89(5): 841-864.

Lee, M. K. O., & Turban, E. 2000. ***A trust model for consumer Internet shopping***. Paper presented at the Meeting of the International Conference on Electronic Commerce 2000 (ICEC2000), Seoul, South Korea.

Li, C., Lim, J.-H., & Wang, Q. 2007. Internal and external influences on IT control governance. ***International Journal of Accounting Information Systems***, 8: 225-229.

Luo, X. M. 2002. Trust production and privacy concerns on the Internet - A framework based on relationship marketing and social exchange theory. ***Industrial Marketing Management***, 31(2): 111-118.

McFadzean, E., Ezingeard, J. N., & Birchall, D. 2007. Perception of risk and the strategic impact of existing IT on information security strategy at board level. ***Online Information Review***, 31: 622-660.

Meinert, D., Peterson, D., Criswell, J., & Crossland, M. 2006. Would Regulation of Web Site Privacy Policy Statements Increase Consumer Trust? ***INFORMING SCIENCE***, 9: 123-142.

Miles, R. E., & Snow, C. C. 1978. ***Organizationa Strategy, Structure, and Process***. New York: McGraw-Hill.

Milne, G. R., & Boza, M.-E. 1998. Trust and concern in consumers' perceptions of marketing information management practices. ***Journal of Interactive Marketing***, 13(1): 5-24.

Mishra, D. P., Heide, J. B., & Cort, S. G. 1998. Information asymmetry and levels of agency relationships. ***Journal of Marketing Research***, 35(3): 277-295.

Mitchell, V. L. 2006. Knowledge integration and information technology project performance. ***MIS Quarterly***, 30(4): 919-939.

Miyazaki, A. D., & Fernandez, A. 2000. Internet privacy and security: An examination of online retailer disclosures. ***Journal of Public Policy & Marketing***, 19(1): 54-61.

Morgan, R. M., & Hunt, S. D. 1994. THE COMMITMENT-TRUST THEORY OF RELATIONSHIP MARKETING. ***Journal of Marketing***, 58(3): 20-38.

Muralidhar, K., Parsa, R., & Sarathy, R. 1999. A general additive data perturbation method for database security. ***Management Science***, 45(10): 1399-1415.

Nagar, V. 2002. Delegation and incentive compensation. ***Accounting Review***, 77(2): 379-395.

Olivero, N., & Lunt, P. 2004. Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. ***Journal of Economic Psychology***, 25(2): 243-262.

Park, J., Shin, S. K., & Sanders, G. L. 2007. Impact of international information technology transfer on national productivity. ***Information Systems Research***, 18(1): 86-102.

Perlman, E. 2007. Topside Turnover, ***Governing***.

Petrison, L. A., & Wang, P. 1993. FROM RELATIONSHIPS TO RELATIONSHIP MARKETING - APPLYING DATABASE TECHNOLOGY TO PUBLIC-RELATIONS. ***Public Relations Review***, 19(3): 235-245.

Pfeffer, J., & Langton, N. 1993. The Effect Of Wage Dispersion On Satisfaction, Productivity, and Working Collaboratively - Evidence From College and University-Faculty. ***Administrative Science Quarterly***, 38(3): 382-407.

Phelps, J., Nowak, G., & Ferrell, E. 2000. Privacy concerns and consumer willingness to provide personal information. ***Journal of Public Policy & Marketing***, 19(1): 27-41.

Phelps, J. E., D'Souza, G., & Nowak, G. J. 2001. Antecedents and Consequences of Consumer Privacy Concerns : An Empirical Investigation. ***Journal of Interactive Marketing***, 14(4).

Posthumus, S., & von Solms, R. 2005. A responsibility framework for information security. ***Security Management, Integrity, and Internal Control in Information Systems***, 193: 205-221.

Preston, D. S., Chen, D., & Leidner, D. E. 2008. Examining the Antecedents and Consequences of CIO Strategic Decision-Making Authority: An Empirical Study. ***Decision Sciences***, 39(4): 605-642.

Raghupathi, W. 2007. Corporate governance of IT: A framework for development. ***Communications of the Acm***, 50(8): 94-99.

Saavedra, E. 1996. Teachers study groups: Contexts for transformative learning and action. ***Theory into Practice***, 35(4): 271-277.

Santalo, J., & Kock, C. J. 2009. Division Director Versus CEO Compensation: New Insights Into the Determinants of Executive Pay. ***Journal of Management***, 35(4): 1047-1077.

Schlosser, A. E., White, T. B., & Lloyd, S. M. 2006. Converting web site visitors into buyers: How web site investment increases consumer trusting beliefs and online purchase intentions. ***Journal of Marketing***, 70(2): 133-148.

SEC. 2005. Staff Statement on Management's Report on Internal Controls Over Financial Reporting: http://www.sec.gov/info/accountants/stafficreporting.htm.

Selnes, F. 1998. Antecedents and consequences of trust and satisfaction in buyer-seller relationships. ***European Journal of Marketing***, 32(3/4): 305-322.

Sheehan, K. B., & Hoy, M. G. 1999. Flaming, complaining, abstaining: How online users respond to privacy concerns. ***Journal of Advertising***, 28(3): 37-51.

Siegel, P. A., & Hambrick, D. C. 2005. Pay disparities within top management groups: Evidence of harmful effects on performance of high-technology firms. ***Organization Science***, 16(3): 259-274.

Sipior, J. C., Ward, B. T., & Rongione, N. M. 2003. Ethics of collecting and using consumer Internet data. ***Information Systems Management***, 21(1): 58-66.

Smaltz, D. H., Sambamurthy, V., & Agarwal, R. 2004. ***The antecedents of CIO role effectiveness in organizations: An empirical study in the healthcare sector***. Paper presented at the Conference on Information Systems and Technology, Denver, CO.

Smith, G. 2004. Sarbanes-oxley: Compliance or sham? ***Journal of Corporate Accounting & Finance***, 15(6): 3 - 5.

Smith, H. J., Milburg, S. J., & Burke, S. J. 1996. Information privacy: Measuring individuals' concerns about organizational practices. ***MIS Quarterly***, 20(2): 167-196.

Staw, B. M. 1980. The Consequences Of Turnover. ***Journal of Occupational Behaviour***, 1(4): 253-273.

Steenkamp, J., & Geyskens, I. 2006. How country characteristics affect the perceived value of web sites. ***Journal of Marketing***, 70(3): 136-150.

Stephens, C. S., Ledbetter, W. N., Mitra, A., & Ford, F. N. 1992a. Executive or Fuctional Manager-The Nature of the CIOs Job. ***MIS Quarterly***, 16(4): 449-467.

Stephens, C. S., Ledbetter, W. N., Mitra, A., & Ford, F. N. 1992b. EXECUTIVE OR FUNCTIONAL MANAGER - THE NATURE OF THE CIOS JOB. ***Mis Quarterly***, 16(4): 449-467.

Stoel, D., & Muhanna, W. A. 2009. IT Internal Control Weaknesses and Firm Performance: An Empirical Investigation.

Straub, D. W., & Welke, R. J. 1998. Coping with systems risk: Security planning models for management decision making. ***MIS Quarterly***, 22(4): 441-469.

Suh, B., & Han, I. 2003. The impact of customer trust and perception of security control on the acceptance of electronic commerce. ***International Journal of Electronic Commerce***, 7(3): 135-161.

Ton, Z., & Huckman, R. S. 2008. Managing the impact of employee turnover on performance: The role of process conformance. ***Organization Science***, 19(1): 56-68.

Turban, E. 2008. ***Information technology for management : transforming organizations in the digital economy***.

Wang, Y. D., & Emurian, H. H. 2005. An overview of online trust: Concepts, elements, and implications. ***Computers in Human Behavior***, 21(1): 105-125.

Wendell, P. J. 2005. SEC staff views on implementation of section 404, Vol. 1: 1-3: SEC Accounting Report.

Yayla, A., & Hu, Q. 2008. Determinants of CIO Compensation Structure and Its Impact on Firm Performance, ***Hawaii International Conference on System Sciences, Proceedings of the 41st Annual***.

Young, E. 2008. Moving Beyound compliance, Global Information Security Survey.

Zhu, K., & Kraemer, K. L. 2002. e-Commerce metrics for net-enhanced organizations: Assessing the value of e-commerce to firm performance in the manufacturing sector. ***Information Systems Research***, 13(3): 275-295.

Appendices

Appendix A. Companies with Information Breach Incidents

No	Event Date	Company Name	Type of Incident	Type of Breaches
1	1/24/2003	SIEBEL SYSTEMS INC	worm	Availability
2	1/28/2003	BOEING CO	worm	Availability
3	1/28/2003	COUNTRYWIDE FINANCIAL CORP	Site attack	Availability
4	1/30/2003	IBM	Data Lost	Confidentiality
5	2/6/2003	BANK OF AMERICA CORP	worm	Integrity
6	2/6/2003	WASHINGTON MUTUAL INC	worm	Availability
7	2/19/2003	AMERICAN EXPRESS CREDIT CORP	Hacking	Confidentiality
8	2/20/2003	MASTERCARD INC	Hacking	Confidentiality
9	4/30/2003	DIRECTV GROUP INC	Hacking	Confidentiality
10	5/8/2003	MICROSOFT CORP	Hacking	Availability
11	6/18/2003	GUESS INC	Program Errors	Confidentiality
12	8/11/2003	ACXIOM CORP	Hacking	Confidentiality
13	8/15/2003	MICROSOFT CORP	worms	Integrity
14	8/21/2003	CSX CORP	virus	Integrity
15	9/10/2003	KNIGHT-RIDDER INC	Site attack	Availability
16	10/1/2003	BEST BUY CO INC	Hacking	Integrity
17	11/22/2003	WELLS FARGO & CO	Data Stolen	Confidentiality
18	11/27/2003	WELLS FARGO & CO	Hacking	Confidentiality
19	12/18/2003	Acxiom Corp.	Data Breach	Confidentiality
20	2/2/2004	GATEWAY INC	System Errors	Confidentiality
21	2/2/2004	IOMEGA CORP	System Errors	Confidentiality
22	2/2/2004	KOHL'S CORP	System Errors	Confidentiality
23	2/2/2004	OPEN SOLUTIONS INC	System Errors	Confidentiality
24	2/2/2004	SAKS INC	System Errors	Confidentiality
25	2/2/2004	TIFFANY & CO	System Errors	Confidentiality
26	2/13/2004	MICROSOFT CORP	Data Lost	Confidentiality
27	3/16/2004	EBAY INC	Hacking	Integrity
28	3/19/2004	BJ'S WHOLESALE CLUB INC	System Errors	Confidentiality
29	4/14/2004	MICROSOFT CORP	Data Breach	Integrity
30	5/18/2004	CISCO SYSTEMS INC	Code Theft	Integrity
31	6/7/2004	LOWE'S COMPANIES INC	Hacking	Confidentiality

32	6/16/2004	AKAMAI TECHNOLOGIES INC	Site attack	Availability
33	6/26/2004	MICROSOFT CORP	Data Stolen	Confidentiality
34	7/14/2004	INTUIT INC	Data Stolen	Confidentiality
35	7/27/2004	GOOGLE INC	Virus	Integrity
36	7/27/2004	YAHOO INC	Virus	Integrity
37	9/28/2004	SUNTRUST BANKS INC	Site attack	Availability
38	10/27/2004	GOOGLE INC	Hacking	Confidentiality
39	11/3/2004	WELLS FARGO & CO	Data Stolen	Confidentiality
40	11/11/2004	AFFILIATED COMPUTER SERVICES	Hacking	Confidentiality
41	12/8/2004	SUNTRUST BANKS INC	Phising	Availability
42	12/27/2004	LYCOS INC	Site attack	Availability
43	2/14/2005	ChoicePoint	Data Breach	Confidentiality
44	2/25/2005	Bank of America	Data Lost	Confidentiality
45	3/5/2005	Automatic Data Processing	Program Errors	Confidentiality
46	3/23/2005	Bank of America,Columbia Funds	Data Breach	Confidentiality
47	3/23/2005	City National Bank	Data Breach	Confidentiality
48	3/23/2005	Nuveen Investments	Data Breach	Confidentiality
49	3/23/2005	Pimco	Data Breach	Confidentiality
50	3/23/2005	U S BANCORP	Data Breach	Confidentiality
51	4/5/2005	MCI	Data Stolen	Confidentiality
52	4/13/2005	Polo Ralph Lauren	Hacking	Confidentiality
53	4/14/2005	COMCAST CORP	illegal data exposed	Confidentiality
54	4/26/2005	Foster Wheeler, Clinton, N.J	Hacking	Confidentiality
55	4/28/2005	Bank of America	Illegal data selling	Confidentiality
56	4/28/2005	Commerce Bank	Illegal data selling	Confidentiality
57	4/28/2005	PNC Bank of Pittsburgh	Illegal data selling	Confidentiality
58	4/28/2005	Wachovia	Illegal data selling	Confidentiality
59	5/2/2005	Time Warner	Data Lost	Confidentiality
60	5/8/2005	IRON MOUNTAIN INC	Data Lost	Confidentiality
61	5/28/2005	Motorola	Data Stolen	Confidentiality
62	6/7/2005	UNITED PARCEL SERVICE INC	Data Lost	Confidentiality
63	6/17/2005	MasterCard International	Hacking	Confidentiality
64	6/21/2005	CVS CAREMARK CORP	System Errors	Confidentiality

65	7/8/2005	IRON MOUNTAIN INC	Data Lost	Confidentiality
66	7/29/2005	EBAY INC	Program Errors	Availability
67	8/8/2005	Huntington National Bank, Toledo, Ohio	Data Stolen	Confidentiality
68	8/8/2005	J.P. Morgan Private Bank.	Data Breach	Confidentiality
69	8/12/2005	VERIZON COMMUNICATIONS INC	Program Errors	Integrity
70	9/22/2005	ChoicePoint	Program Errors	Confidentiality
71	9/23/2005	Bank of America	Data Stolen	Confidentiality
72	10/8/2005	BLOCKBUSTER INC	Data Lost	Confidentiality
73	11/5/2005	SAFEWAY INC	Data Stolen	Confidentiality
74	11/7/2005	PAPA JOHNS INTERNATIONAL INC	Program Errors	Confidentiality
75	11/18/2005	Boeing Co	Data Stolen	Confidentiality
76	12/6/2005	SAM'S CLUB	Program Errors	Integrity
77	12/21/2005	Ford Motor Co	Data Stolen	Confidentiality
78	12/22/2005	H&R Block	Program Errors	Confidentiality
79	12/25/2005	Convergys	Program Errors	Integrity
80	12/27/2005	Marriott International	Data Lost	Confidentiality
81	1/1/2006	Progressive Casualty Insurance	Data Breach	Confidentiality
82	1/2/2006	H&R Block	Program Errors	Integrity
83	1/11/2006	UNITED PARCEL SERVICE INC	Data Lost	Confidentiality
84	1/20/2006	Honeywell International	Data Breach	Confidentiality
85	1/25/2006	Ameriprise Financial	Data Stolen	Confidentiality
86	1/31/2006	FedEx Freight West.	System Errors	Integrity
87	2/1/2006	Automatic Data Processing	Data Breach	Confidentiality
88	2/6/2006	Regions Bank	System Errors	Confidentiality
89	2/14/2006	BANK OF AMERICA CORP	Data Stolen	Confidentiality
90	2/14/2006	OFFICEMAX INC	Hacking	Confidentiality
91	2/14/2006	WASHINGTON MUTUAL INC	Hacking	Confidentiality
92	2/14/2006	WELLS FARGO & CO	Hacking	Confidentiality
93	2/17/2006	McAfee	Data Lost	Confidentiality
94	2/20/2006	Verizon Communications Inc.(Alltel Corporation)	Data Lost	Confidentiality

95	3/1/2006	American Insurance Group (AIG)	Hacking	Confidentiality
96	3/1/2006	MEDCO HEALTH SOLUTIONS INC	Data Stolen	Confidentiality
97	3/1/2006	Verizon Communications	Data Stolen	Confidentiality
98	3/13/2006	General Motors	Hacking	Confidentiality
99	4/3/2006	AUTHORIZE.NET HOLDINGS INC	Data Stolen	Confidentiality
100	4/6/2006	Iron Mountain / Long Island Railroad	Data Lost	Confidentiality
101	4/7/2006	Fifth Third Bank	Data Breach	Confidentiality
102	4/26/2006	MASTERCARD INC	Hacking	Availability
103	4/26/2006	MORGAN STANLEY	Data Breach	Confidentiality
104	4/29/2006	Union Pacific Corporation	Data Stolen	Confidentiality
105	5/1/2006	Equifax	Data Stolen	Confidentiality
106	5/5/2006	Wells Fargo	Data Stolen	Confidentiality
107	5/6/2006	Mercantile Bank shares	Data Stolen	Confidentiality
108	6/2/2006	ELECTRONIC DATA SYSTEMS CORP	Data Stolen	Confidentiality
109	6/27/2006	AAAAA Rent-A-Space	Data Breach	Confidentiality
110	6/29/2006	AllState Insurance	Data Breach	Confidentiality
111	7/5/2006	BISYS GROUP INC	Data Lost	Confidentiality
112	7/6/2006	AUTOMATIC DATA PROCESSING	Data Breach	Integrity
113	7/26/2006	Netscape.com	Hacking	Availability
114	8/1/2006	Affiliated Computer Services, Inc	Program Errors	Confidentiality
115	8/1/2006	DOLLAR TREE INC	System Errors	Integrity
116	8/1/2006	U S BANCORP	Data Breach	Confidentiality
117	8/1/2006	Weyerhaeuser	Data Breach	Confidentiality
118	8/1/2006	Williams Sonoma, Inc	Data Stolen	Integrity
119	8/8/2006	LINENS N THINGS INC	Data Breach	Integrity
120	8/14/2006	Chevron	Data Stolen	Confidentiality
121	8/21/2006	Sovereign Bank	Data Stolen	Confidentiality
122	8/23/2006	Xerox	Data Stolen	Confidentiality
123	8/25/2006	Verizon Wireless	Data Breach	Integrity
124	8/27/2006	AT&T	Hacking	Availability
125	8/28/2006	Wells Fargo	Data Stolen	Confidentiality
126	9/7/2006	Chase Card Services	Data Lost	Confidentiality
127	9/24/2006	General Electric Co	Data Stolen	Confidentiality
128	10/1/2006	Gymboree	Site attack	Availability

129	10/1/2006	TD Ameritrade Holding Corp	Hacking	Integrity
130	10/26/2006	Aetna	Data Stolen	Confidentiality
131	11/3/2006	Starbucks	Data Stolen	Confidentiality
132	12/12/2006	Money Gram International	Data Breach	Availability
133	12/14/2006	Bank of America	Data Breach	Integrity
134	12/14/2006	Boeing	Data Stolen	Confidentiality
135	12/20/2006	TJX	Data Breach	Confidentiality
136	12/29/2006	KEYCORP	Data Stolen	Confidentiality
137	1/12/2007	KB Home	Data Stolen	Confidentiality
138	1/19/2007	Electronic Data Systems-EDS	Data Stolen	Confidentiality
139	1/23/2007	XEROX CORP	Data Stolen	Confidentiality
140	1/26/2007	Chase/Bank One	Illegal data selling	Confidentiality
141	2/1/2007	Washington Mutual	Hacking	Integrity
142	2/23/2007	IBM	Data Lost	Confidentiality
143	3/14/2007	WELLPOINT INC	Data Stolen	Confidentiality
144	3/28/2007	RadioShack	Data Lost	Confidentiality
145	4/1/2007	Bank of America	Data Stolen	Confidentiality
146	4/1/2007	Caterpillar Inc.	Data Stolen	Confidentiality
147	4/1/2007	Life Time Fitness	Data Stolen	Confidentiality
148	4/7/2007	AOL	Hacking	Integrity
149	4/15/2007	JP Morgan Chase	Data Breach	Confidentiality
150	4/17/2007	CVS CAREMARK CORP	Data Breach	Confidentiality
151	4/27/2007	Google	Hacking	Integrity
152	5/15/2007	Columbia Bank	Hacking	Integrity
153	5/19/2007	Texas First Bank- S1 Corp	Data Stolen	Confidentiality
154	5/25/2007	Pfizer	Data Stolen	Integrity
155	5/28/2007	Dollar General	Data Breach	Integrity
156	5/29/2007	GfK Custom Research North	Data Stolen	Availability
157	5/29/2007	SAIC	Data Breach	Integrity
158	6/3/2007	Fidelity National Information	Data Breach	Confidentiality
159	6/11/2007	PFIZER INC	Data Stolen	Confidentiality
160	6/21/2007	AMERICAN AIRLINES INC	Data Breach	Confidentiality
161	7/6/2007	Western Union	Hacking	Confidentiality
162	7/25/2007	Merrill Lynch	Data Stolen	Confidentiality
163	7/27/2007	AT&T	Data Stolen	Integrity
164	7/31/2007	Textron	Data Stolen	Confidentiality
165	8/6/2007	VERISIGN INC	Data Stolen	Confidentiality
166	8/7/2007	Electronic Data Systems	Data Breach	Integrity
167	9/10/2007	Wachovia Bank	Data Breach	Integrity

168	9/12/2007	UNITEDHEALTH GROUP INC	Data Lost	Confidentiality
169	9/14/2007	TD AMERITRADE HOLDING CORP	Hacking	Confidentiality
170	9/19/2007	Gap Inc.	Data Stolen	Confidentiality
171	9/20/2007	Semtech	Data Lost	Confidentiality
172	9/25/2007	E-Bay	Site attack	Availability
173	9/25/2007	Pfizer- Wheels, Inc.	Program Errors	Confidentiality
174	10/1/2007	Citibank	Hacking	Availability
175	10/10/2007	Commerce Bank	Hacking	Integrity
176	10/15/2007	Home Depot, Massachusetts	Data Stolen	Confidentiality
177	10/16/2007	ADMINISTAFF INC	Data Stolen	Integrity
178	10/22/2007	Blockbuster	Data Lost	Confidentiality
179	10/30/2007	HARTFORD FINANCIAL SERVICES	Data Breach	Availability
180	11/28/2007	Oracle Corporation	Data Lost	Confidentiality
181	12/1/2007	WA Bank of America	Data Breach	Confidentiality
182	12/3/2007	Wendy's International	Data Stolen	Confidentiality
183	12/21/2007	GENERAL ELECTRIC CO	Data Lost	Confidentiality
184	12/21/2007	IRON MOUNTAIN INC	Data Lost	Confidentiality
185	12/21/2007	Iron Mountain-GE Money-Americas	Data Lost	Confidentiality
186	1/1/2008	People's United Bank	Data Lost	Confidentiality
187	1/8/2008	Google Website	Hacking	Confidentiality
188	1/15/2008	Kraft Foods	Data Stolen	Confidentiality
189	1/31/2008	Marriott International - Hewitt	Data Lost	Confidentiality
190	2/10/2008	Old Navy	Data Breach	Integrity
191	2/16/2008	Genworth Life and Annuity Insurance Co	Data Breach	Confidentiality
192	2/18/2008	Stryker Instruments	Hacking	Confidentiality
193	2/20/2008	3M Company	Data Stolen	Confidentiality
194	3/1/2008	Agilent -Stock & Option Solutions	Data Stolen	Confidentiality
195	3/5/2008	SunGard Availability Services (SAS) #2	Data Lost	Confidentiality
196	3/8/2008	Viacom Inc.(MTV Network)	Data Breach	Confidentiality
197	4/1/2008	Pfizer Inc	Data Stolen	Integrity
198	4/8/2008	WELLCARE HEALTH PLANS INC	Program Errors	Confidentiality
199	4/8/2008	WELLPOINT INC	Data Breach	Confidentiality

200	4/10/2008	Community Bank	Data Breach	Confidentiality
201	4/10/2008	H&R Block	Data Breach	Integrity
202	4/22/2008	Verizon Wireless	Data Breach	Confidentiality
203	4/23/2008	First Bank and Trust	Data Breach	Confidentiality
204	4/29/2008	Merrill Corporation	Program Errors	Confidentiality
205	5/1/2008	Adobe Systems Inc	Data Breach	Integrity
206	5/1/2008	BB&T CORP	Data Stolen	Confidentiality
207	5/11/2008	SunGard Data Systems/ Newedge	Data Breach	Confidentiality
208	5/15/2008	AT&T	Data Stolen	Confidentiality
209	5/16/2008	Wells Fargo	Data Breach	Integrity
210	5/27/2008	Charter Communications	Data Breach	Availability
211	6/9/2008	United Transportation Union	Data Lost	Confidentiality
212	7/1/2008	Wells Fargo	Data Breach	Integrity
213	7/15/2008	Charter Communications	Data Stolen	Confidentiality
214	7/17/2008	BRISTOL-MYERS SQUIBB CO	Data Breach	Confidentiality
215	7/25/2008	Delphi	Data Lost	Confidentiality
216	7/30/2008	United Bancorp of WY-Parent Company	Data Lost	Confidentiality
217	8/1/2008	American Greetings / UPS	Data Breach	Integrity
218	8/7/2008	Bank of America	Data Stolen	Confidentiality
219	8/23/2008	Wells Fargo #2	Data Lost	Confidentiality
220	8/28/2008	Cape Coral Wachovia Bank	Data Lost	Confidentiality
221	8/29/2008	Bear, Stearns Corp, JP Morgan Chase	Program Errors	Confidentiality
222	9/2/2008	Keizer Lowe's	Data Breach	Confidentiality
223	9/10/2008	COUNTRYWIDE FINANCIAL CORP	Data Breach	Confidentiality
224	9/21/2008	Bank of America	System Errors	Integrity
225	9/24/2008	Rite Aid	Data Lost	Confidentiality
226	10/17/2008	Community Bank	Program Errors	Confidentiality
227	10/18/2008	Symantec	Data Stolen	Confidentiality
228	10/29/2008	Starbucks Corp	Data Stolen	Confidentiality
229	11/13/2008	Pulte Homes Las Vegas	Data Breach	Confidentiality
230	12/3/2008	Hewlett Packard	Data Stolen	Confidentiality
231	12/8/2008	Bank of America	Hacking	Integrity
232	12/10/2008	Regions Bank	Data Stolen	Confidentiality

Appendix B. Companies with IT Internal Control Weaknesses

No	Year	GVKEY	Company Name	Types of IT Internal Control Weaknesses
1	2004	001487	AMERICAN INTERNATIONAL GROUP	Reliability Control issues
2	2004	002222	SAVIENT PHARMACEUTICALS INC	Control issues
3	2004	002290	OFFICEMAX INC	Control issues
4	2004	002497	MASTEC INC	Integrity Availability
5	2004	003734	DANA HOLDING CORP	Reliability
6	2004	004108	FLOWSERVE CORP	Reliability Integrity Availability Control issues
7	2004	004194	EASTMAN KODAK CO	Integrity Availability
8	2004	004242	EL PASO CORP	Integrity Availability Control issues
9	2004	004601	FANNIE MAE	Confidentiality Reliability Integrity Availability Control issues
10	2004	004622	FERRO CORP	Integrity Availability
11	2004	005234	GOODYEAR TIRE & RUBBER CO	Control issues
12	2004	006136	INTERPUBLIC GROUP OF COS	Reliability Integrity Availability Control issues
13	2004	007085	MASCO CORP	Control issues
14	2004	007152	MCDERMOTT INTL INC	Integrity Availability Control issues
15	2004	007991	TEREX CORP	Control issues
16	2004	008001	NORTHWESTERN CORP	Confidentiality Control issues
17	2004	008716	PREPAID LEGAL SERVICES INC	Integrity Availability
18	2004	009611	SERVICE CORP INTERNATIONAL	Integrity Availability Control issues
19	2004	010000	STANDARD MOTOR PRODS	Integrity Availability
20	2004	010386	TECUMSEH PRODUCTS CO -CL A	Integrity Availability Control issues
21	2004	010991	SCIENTIFIC GAMES CORP	Material weakness
22	2004	012589	HEALTHSOUTH CORP	Reliability Integrity Availability Control issues
23	2004	013354	AUDIOVOX CORP -CL A	Integrity Availability Control issues
24	2004	014820	PRESIDENTIAL LIFE CORP	Control issues
25	2004	014908	PRIDE INTERNATIONAL INC	Integrity Availability
26	2004	016650	RTI INTL METALS INC	Confidentiality Integrity Availability Control issues
27	2004	017070	NATIONAL PENN BANCSHARES INC	Reliability Control issues

28	2004	021232	NTN BUZZTIME INC	Control issues
29	2004	023291	BIOLASE TECHNOLOGY INC	Integrity Availability Control issues
30	2004	023700	ZILOG INC	Control issues
31	2004	024216	AES CORP. (THE)	Integrity Availability
32	2004	024678	HORACE MANN EDUCATORS CORP	Control issues
33	2004	028758	SPSS INC	Integrity Availability
34	2004	029108	PATTERSON-UTI ENERGY INC	Reliability
35	2004	030298	HIGHWOODS PROPERTIES INC	Integrity Availability
36	2004	061562	ADVANCED ENERGY INDS INC	Integrity Availability Control issues
37	2004	062922	99 CENTS ONLY STORES	Integrity Availability Control issues
38	2004	063099	BROADVISION INC	Integrity Availability
39	2004	064135	DELTIC TIMBER CORP	Control issues
40	2004	064699	FLAGSTAR BANCORP INC	Integrity Availability
41	2004	066065	UNITED RENTALS INC	Reliability Control issues
42	2004	113491	GLOBAL CROSSING LTD	Integrity Availability
43	2004	124358	INTERNAP NETWORK SVCS CORP	Control issues
44	2005	001072	AVX CORP	Integrity Availability Control issues
45	2005	001410	ABM INDUSTRIES INC	Control issues
46	2005	002222	SAVIENT PHARMACEUTICALS INC	Control issues
47	2005	002269	BLOCK H & R INC	Reliability
48	2005	003310	CA INC	Reliability
49	2005	003734	DANA HOLDING CORP	Reliability Integrity Availability Control issues
50	2005	003971	DIONEX CORP	Control issues
51	2005	004108	FLOWSERVE CORP	Integrity Availability Control issues
52	2005	004390	ENNIS INC	Integrity Availability
53	2005	004601	FANNIE MAE	Integrity Availability Control issues
54	2005	004622	FERRO CORP	Integrity Availability
55	2005	004918	FROZEN FOOD EXPRESS INDS	Integrity Availability
56	2005	006081	NAVISTAR INTERNATIONAL CORP	Reliability Integrity Availability Control issues
57	2005	006136	INTERPUBLIC GROUP OF COS	Integrity Availability Control issues
58	2005	008092	BRISTOW GROUP INC	Confidentiality Reliability Control issues
59	2005	008151	ONEOK INC	Integrity Availability
60	2005	008240	PHH CORP	Reliability Control issues

61	2005	010386	TECUMSEH PRODUCTS CO -CL A	Integrity Availability Control issues
62	2005	012262	ASTEC INDUSTRIES INC	Integrity Availability
63	2005	012589	HEALTHSOUTH CORP	Integrity Availability Control issues
64	2005	013375	GENERAL COMMUNICATION -CL A	Integrity Availability
65	2005	014268	BORLAND SOFTWARE CORP	Reliability
66	2005	014908	PRIDE INTERNATIONAL INC	Reliability
67	2005	016821	FIRST BANCORP P R	Reliability
68	2005	023810	ION GEOPHYSICAL CORP	Reliability
69	2005	025234	BUCKLE INC	Integrity Availability Control issues
70	2005	026523	NYFIX INC	Reliability Integrity Availability Control issues
71	2005	027760	NAUTILUS INC	Integrity Availability
72	2005	029108	PATTERSON-UTI ENERGY INC	Reliability Control issues
73	2005	029709	SONIC SOLUTIONS	Integrity Availability Control issues
74	2005	030298	HIGHWOODS PROPERTIES INC	Integrity Availability
75	2005	060992	MEMC ELECTRONIC MATRIALS INC	Control issues
76	2005	062984	TITANIUM METALS CORP	Integrity Availability
77	2005	064156	MONSTER WORLDWIDE INC	Reliability
78	2005	064630	TAKE-TWO INTERACTIVE SFTWR	Integrity Availability
79	2005	065421	FARO TECHNOLOGIES INC	Confidentiality
80	2005	065570	AMER ITALIAN PASTA CO -CL A	Confidentiality Reliability
81	2005	066708	BROADCOM CORP -CL A	Reliability
82	2005	122394	PERFICIENT INC	Integrity Availability Control issues
83	2005	133767	KRISPY KREME DOUGHNUTS INC	Reliability Control issues
84	2005	145041	BIG 5 SPORTING GOODS CORP	Control issues
85	2006	002577	CTS CORP	Integrity Availability
86	2006	003310	CA INC	Reliability
87	2006	003734	DANA HOLDING CORP	Control issues
88	2006	004601	FANNIE MAE	Confidentiality Integrity Availability Material weakness
89	2006	004807	FLOW INTL CORP	Reliability Control issues Material weakness
90	2006	006136	INTERPUBLIC GROUP OF	Integrity Availability Material weakness

			COS	
91	2006	008240	PHH CORP	Integrity Availability Control issues
92	2006	008333	PAR PHARMACEUTICAL COS INC	Integrity Availability
93	2006	009599	SEMTECH CORP	Reliability
94	2006	010549	THOR INDUSTRIES INC	Integrity Availability Control issues
95	2006	012669	CARMIKE CINEMAS INC	Integrity Availability
96	2006	013184	CYTRX CORP	Integrity Availability
97	2006	014256	MAXIM INTEGRATED PRODUCTS	Reliability
98	2006	014268	BORLAND SOFTWARE CORP	Reliability
99	2006	024782	PERRIGO CO	Integrity Availability Control issues
100	2006	025783	MCAFEE INC	Reliability
101	2006	026015	TRIDENT MICROSYSTEMS INC	Reliability Control issues
102	2006	026523	NYFIX INC	Integrity Availability
103	2006	028139	SANMINA-SCI CORP	Control issues
104	2006	029241	JDS UNIPHASE CORP	Integrity Availability
105	2006	030697	AFFILIATED COMPUTER SERVICES	Reliability
106	2006	062922	99 CENTS ONLY STORES	Integrity Availability
107	2006	062967	SUNRISE SENIOR LIVING INC	Reliability
108	2006	064766	RAMBUS INC	Integrity Availability
109	2006	065570	AMER ITALIAN PASTA CO -CL A	Confidentiality
110	2006	065706	ABOVENET INC	Integrity Availability
111	2006	133767	KRISPY KREME DOUGHNUTS INC	Reliability Integrity Availability Control issues
112	2006	145041	BIG 5 SPORTING GOODS CORP	Integrity Availability Control issues
113	2007	003946	DIEBOLD INC	Reliability Integrity Availability
114	2007	004622	FERRO CORP	Integrity Availability
115	2007	006081	NAVISTAR INTERNATIONAL CORP	Integrity Availability Control issues
116	2007	006109	INTL RECTIFIER CORP	Reliability Integrity Availability Control issues
117	2007	007762	NATIONAL PRESTO INDS INC	Confidentiality
118	2007	007974	NISOURCE INC	Integrity Availability
119	2007	008333	PAR PHARMACEUTICAL COS INC	Material weakness
120	2007	008512	PETROLEUM DEVELOPMENT CORP	Integrity Availability

121	2007	012603	CONSECO INC	Integrity Availability
122	2007	012669	CARMIKE CINEMAS INC	Integrity Availability
123	2007	013375	GENERAL COMMUNICATION	Integrity Availability
124	2007	014256	MAXIM INTEGRATED PRODUCTS	Reliability
125	2007	014489	DELL INC	Reliability Integrity Availability
126	2007	024473	SEPRACOR INC	Integrity Availability
127	2007	025783	MCAFEE INC	Material weakness
128	2007	026015	TRIDENT MICROSYSTEMS INC	Reliability Control issues
129	2007	029211	BOSTON PRIVATE FINL HOLDINGS	Reliability Control issues
130	2007	029755	BEAZER HOMES USA INC	Reliability
131	2007	031564	ACI WORLDWIDE INC	Integrity Availability
132	2007	061181	INTEGRA LIFESCIENCES HLDGS	Integrity Availability Control issues
133	2007	062967	SUNRISE SENIOR LIVING INC	Reliability Integrity Availability Material weakness
134	2007	065430	CHILDRENS PLACE RETAIL STRS	Reliability Integrity Availability
135	2007	065570	AMER ITALIAN PASTA CO -CL A	Confidentiality
136	2007	065706	ABOVENET INC	Integrity Availability
137	2007	128759	NATCO GROUP INC	Confidentiality
138	2007	133767	KRISPY KREME DOUGHNUTS INC	Integrity Availability Control issues
139	2007	160600	SYMMETRY MEDICAL INC	Reliability Integrity Availability Control issues
140	2007	162264	NEENAH PAPER INC	Integrity Availability
141	2007	260778	WELLCARE HEALTH PLANS INC	Confidentiality Reliability Control issues
142	2008	003946	DIEBOLD INC	Reliability Integrity Availability
143	2008	004601	FANNIE MAE	Confidentiality Integrity Availability
144	2008	006081	NAVISTAR INTERNATIONAL CORP	Control issues
145	2008	006109	INTL RECTIFIER CORP	Integrity Availability Control issues
146	2008	007486	MODINE MANUFACTURING CO	Reliability
147	2008	009355	SAFEGUARD SCIENTIFICS INC	Integrity Availability
148	2008	009611	SERVICE CORP INTERNATIONAL	Integrity Availability
149	2008	012603	CONSECO INC	Integrity Availability
150	2008	013375	GENERAL	Integrity Availability

			COMMUNICATION	
151	2008	017070	NATIONAL PENN BANCSHARES INC	Integrity Availability Control issues
152	2008	029353	SHAW GROUP INC	Integrity Availability
153	2008	062922	99 CENTS ONLY STORES	Integrity Availability
154	2008	065570	AMER ITALIAN PASTA CO	Confidentiality
155	2008	065706	ABOVENET INC	Integrity Availability
156	2008	147305	JETBLUE AIRWAYS CORP	Integrity Availability
157	2008	162264	NEENAH PAPER INC	Integrity Availability
158	2008	177264	COVIDIEN LTD	Integrity Availability

Appendix C. Survey Questions

Now we would like to get your thoughts about Internet privacy. For the following statements, please indicate your level of agreement (Q1 ~ Q6).
1= Strongly Disagree, 2= Disagree, 3= Neutral 4= Agree, 5= Strongly Agree

Q1. Websites use my personal information only for the authorized purposes.

Q2. I think a web site fulfills its obligation in privacy and security on both transactions and operations, according to it privacy and security statements.

Q3. I think that protecting personal information is more important that convenience such as personalized services, when I visit a web site.

Q4. A website uses my information only for the authorized purposes, when the website explicitly expresses why it request a particular type of personal information such as contact, demographic, and financial information.

Q5. A website uses my information only for the authorized purposes, although the website collects my browsing habits without any notice.

Q6. When you visit or register a website, how well do you understand its privacy statement? Would you say that . . .
- o I have never read it
- o I read it, but I did not understand it
- o I have a limited understanding of it
- o I understand it
- o I understood and keep track of changes

Q7. When I visit or register at a website, I am aware if they have third party privacy seals such as TRUSTe, WebTrust and BBB *Online*.

Q8. Are you aware of what kind of behavioral information a web site collect from your browser according to your cookie preference?
- o Yes
- o No

Q9. In the past, how many times have you encountered personal information misuse? Would you say . . .
- o 0 times
- o 1 ~ 2 times
- o 3 ~ 5 times
- o 6 ~ 10 times
- o More than 10 times

Q10. In terms of hours, how long do you use websites such as Google, Yahoo, Amazon.com, Chase.com and CNN.com?

- o Never
- o Less than one hour per week
- o 1 to under 5 hours per week
- o 5 to under 15 hours per week
- o 15 hours or more per week

Now we want to ask you about providing various types of information on a website. Personal information can be categorized into **contact information** (name, email, address, telephone), **demographic information** (gender, marital status, ethnicity, country of residence, occupation), **behavioral information** (browsing habits), and **financial information** (credit card, bank account). Please indicate the extent to which you, as an individual, agree or disagree with providing the type of personal information in the statements for websites you *frequently* visit.

Q11. I am willing to provide the following personal information for **search engine websites** (e.g., Google, Yahoo). Please check all that apply.

	Very Likely	**Slightly Likely**	**Neutral**	**Slightly Unlikely**	**Very Unlikely**
Contact (e.g ., name, email, address, telephone)	5	4	3	2	1
Demographic (e.g., gender, marital status, ethnicity, country of residence, occupation)	5	4	3	2	1
Browsing habits (e.g., my browsing history)	5	4	3	2	1
Financial (e.g., credit card, bank account)	5	4	3	2	1

Q12. I am willing to provide the following information for **online retailers** (e.g., Amazon, buy.com). Please check all that apply.

	Very Likely	**Slightly Likely**	**Neutral**	**Slightly Unlikely**	**Very Unlikely**
Contact (e.g ., name, email, address, telephone)	5	4	3	2	1
Demographic (e.g., gender, marital status, ethnicity, country of residence, occupation)	5	4	3	2	1
Browsing habits (e.g., my browsing history)	5	4	3	2	1
Financial (e.g., credit card, bank account)	5	4	3	2	1

Appendix D. Correlation with Search Engines

	Mean	S.D.	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	x_{13}	x_{14}
x_1	1.656	0.471	1													
x_2	1.521	0.460	.733**	1												
x_3	0.942	0.391	.579**	.686**	1											
x_4	0.788	0.364	.354**	.289**	.359**	1										
x_5	3.653	1.620	-.110**	-0.04	-.089*	-.151**	1									
x_6	3.648	1.455	-.231**	-.186**	-.186**	-.222**	.263**	1								
x_7	3.311	1.567	-.084*	-.072*	-.137**	-.111**	.338**	.314**	1							
x_8	3.415	1.451	-.074*	-.092*	-.113**	-.076*	.070*	.152**	.119**	1						
x_9	3.035	1.378	-.288**	-.351**	-.293**	-.202**	.223**	.490**	.299**	.176**	1					
x_{10}	2.877	1.751	-.103**	-.134**	-.096**	0	.183**	.275**	.324**	0.069	.307**	1				
x_{11}	2.879	1.686	-.103**	-.165**	-.107**	-0.05	.190**	.338**	.321**	.140**	.367**	.616**	1			
x_{12}	1.729	0.967	-0.067	-.139**	-0.019	0.033	.149**	.237**	.225**	.199**	.288**	.340**	.300**	1		
x_{13}	3.333	1.249	0.04	0.009	0.055	0.041	.085*	.103**	.101**	.200**	.131**	0.056	.085*	.085*	1	
x_{14}	2.760	2.307	-.128**	-0.053	-.102**	-0.04	.123**	.191**	.235**	.140**	.367**	.148**	.209**	.224**	.164**	1

Appendix E. Correlation with Online Retailers

	Mean	S.D.	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	x_{13}	x_{14}
x_1	1.228	0.431	1													
x_2	1.521	0.460	.812**	1												
x_3	1.019	0.403	.597**	.679**	1											
x_4	0.257	0.221	.596**	.520**	.478**	1										
x_5	3.653	1.620	-0.043	-0.033	-0.056	-0.031	1									
x_6	3.648	1.455	-.201**	-.181**	-.150**	-.249**	.263**	1								
x_7	3.311	1.567	-.166**	-.175**	-.147**	-.168**	.338**	.314**	1							
x_8	3.415	1.451	-0.062	-.081*	-.099**	-.079*	.070*	.152**	.119**	1						
x_9	3.035	1.378	-.334**	-.313**	-.286**	-.299**	.223**	.490**	.299**	.176**	1					
x_{10}	2.877	1.751	-.206**	-.181**	-.108**	-.128**	.183**	.275**	.324**	0.069	.307**	1				
x_{11}	2.879	1.686	-.239**	-.191**	-.121**	-.178**	.190**	.338**	.321**	.140**	.367**	.616**	1			
x_{12}	1.729	0.967	-.180**	-.171**	-0.045	-.118**	.149**	.237**	.225**	.199**	.288**	.340**	.300**	1		
x_{13}	3.333	1.249	-0.007	0.003	0.055	0.029	.085*	.103**	.101**	.200**	.131**	0.056	.085*	.085*	1	
x_{14}	2.760	2.307	-.142**	-.093**	-.108**	-.099**	.123**	.191**	.235**	.140**	.367**	.148**	.209**	.224**	.164**	1